ZKAccess User Manual

Version: 1.1

Software Version: For ZKAccess 4.1.8/5.0.8 and above Version

Date: June, 2011

About This Manual

This document introduces the main functions, the user interface and operations of the system. For installation, please refer to the Quick Installation Guide.

Table of Contents

Definitions ii

1. System Instruction 1

1.1 Functions Instruction 1
1.2 Basic Operation Flow 1

2. System Management 3

3. My Work Panel 5

4. Personnel System Management 6

4.1 Department Management 6
4.2 Personnel Management 6
4.2.1 Add Personnel 7
4.2.2 Personnel Information Maintenance 8
4.2.3 Personnel Adjustment 10

5. Device Management 11

5.1 Area Settings 11
5.2 Device Management 11
5.2.1 Add Access Control Panel 11
5.2.2 Add Network Video Recorder (For Professional Version 5.0.8 and above) 14
5.2.3 Device Maintenance 14
5.3 Device Communication Management 14
5.4 Daylight Saving Time 15

6. Security System Management 17

6.1 Access Control Time Zones 17
6.2 Access Control Holidays 18
6.3 Door Settings 19
6.3.1 Door Management 20
6.3.2 First-Card Normal Open 23
6.3.3 Multi-Card Opening 23
6.3.4 Interlock Settings 24
6.3.5 Anti-pass Back Settings 25
6.3.6 Linkage Setting 25
6.4 Access Levels 27
6.5 Personnel Access Levels 27
6.6 Real-time Monitoring 28
6.7 Access Control Reports 33

7. Video System (For Professional Version 5.0.8 and above) 35

8. System Settings 37

8.1 User Management 37
8.2 Database Management 38
8.3 System Parameters 40
8.4 Log Records 40

9. Appendices 41

Appendix 1 Common Operation 41
Appendix 2 END-USER LICENSE AGREEMENT FOR THIS SOFTWARE 46
Appendix 3 FAQs 48

Definitions

Super User: The user who has all operation levels of the system, who can assign new users (such as company management personnel, registrar, and access control administrator) in the system and configure the roles of corresponding users.

Role: During daily use, the super user needs to assign new users having different levels. To avoid setting individual levels for each user, roles having certain levels can be defined in Role Management, and then assigned to specified users.

Access Control Time Zone: It can be used for door timing. The reader can be made usable during valid time periods for certain doors and unusable during other time periods. Time zone can also be used to set Normal Open time periods for doors or set access control levels so that specified users can only access specified doors during specified time periods (including access levels and First-Card Normal Open settings).

Door Status Delay: The duration for delayed detection of the door sensor after the door is opened. Detection is performed only after the door is opened and the delay duration expired. When the door is not in the “Normally Open” period, and the door is opened, the device will start timing. It will trigger the alarm when the delay duration expires, and stop alarming when the door is closed. The door status delay should be longer than the lock drive duration.

Close and Reverse-lock: Set whether or not to lock after door closing.

Lock Drive Duration: Used to control the delay for unlocking after card punching.

First-Card Normal Open: During a specified interval, after the first verification by the person having First-Card Normal Open level, the door will be Normal Open, and will automatically restore closing after the valid interval expires.

Multi-Card Opening: This function needs to be enabled in some special access occasions where the door will open only after the consecutive verification of multiple people. Any person verifying outside of the defined combination (even if the person belongs to other combinations) will interrupt the procedure, requiring a 10 seconds wait to restart verification. It will not open by verification of only one of the combination.

Interlock: Can be set for any two or more locks belonging to one access control panel, so that when one door is opened, the others will be closed, allowing only one door to be open at a time.

Anti-pass Back: The card holder who entered from a door by card punching must exit from the same door by card punching, with the entry and exit records strictly consistent.

Linkage Setting: When an event is triggered at an input point of the access control system, a linkage action will occur at the specified output point to control such events as verification, opening, alarming and exception of the system and list them in the corresponding monitored report for view by the user.

1. System Instruction

1.1 Functions Instruction

Security management has increasing concerns for modern enterprises. This management system helps customers to integrate safety procedures on one platform, making access control management easier and more practical so as to improve efficiency.

❁ **System Features**

1. Powerful data processing capacity, allowing the management of access control data for 30,000 people.

2. Visible and reasonable work flows come from abundant experience in access control management.

3. Automatic user name list management.

4. Multilevel, role-based, management secures user data confidentiality.

5. Real-time data acquisition system ensures prompt feedback of access control data to management.

❁ **Configuration Requirements:**

CPU: Master frequency of 2.0G or above;

Memory: 1G or above;

Hardware: Available space of 10G or above. **We recommend using NTFS hard disk partition as the software installation directory (NTFS hard disk partition has the better performance and higher security)**.

❁ **Operating System:**

Supported Operating Systems:

Windows XP/Windows 2003/Windows Vista/Windows 7

Supported Databases:

MySQL/MS SQL Server 2005/Oracle10g

❁ **System Modules:**

The system includes five major functional modules:

Personnel System: Primarily two parts: first, Department Management settings, used to set the company's organizational chart; second, Personnel Management settings, used to input personnel information, assign departments, maintain and manage personnel.

Device System: Set communication parameters for device connection, including system settings and machine settings. After successful communication, the information of connected devices can be viewed and operations such as remote monitoring, uploading and downloading can be performed in the system.

Access Control System: WEB-based management system enabling normal access control functions, management of networked access control panel via computer, and unified personnel access management. The access control system sets door opening time and levels for registered users so that some users are permitted to unlock some doors through verification during certain intervals.

Video System (for professional version): The system provides the video linkage function to manage the network video recorder, view the real-time video, and query the video records. It opens the Real-time Video when the linkage events happen.

System Settings: Primarily used to assign system users and configure the roles of corresponding modules; database management such as backup, initialization and recovery; set system parameters and manage system operation logs.

1.2 Basic Operation Flow

The following are the basic steps to use the system, based on the role of a super user. Different users have different operation levels, so the steps may slightly differ. The user just needs to follow the steps below and skip the items which are not displayed on their interface.

Step 1: Log in to the system to modify the default password of the account;

Step 2: Assign accounts and roles to system users (such as management personnel, registrar, access control administrator);

Step 3: Set system parameters, database, notice, reminder and other frequently used system information;

Step 4: Add devices to the system and configure the basic information of devices;

Step 5: The user sets departmental organization chart (refer to the organizational chart of your company);

Step 6: Input company personnel and conduct daily maintenance of the personnel;

Step 7: Set access control time zones and access control holidays (as access control exceptions);

Step 8: Set parameters for access controlled doors;

Step 9: Set access levels to establish access control based on door group and time zones;

Step 10: Set the access levels of personnel by assigning personnel to access levels to decide which people can open which doors during which time zones.

2. System Management

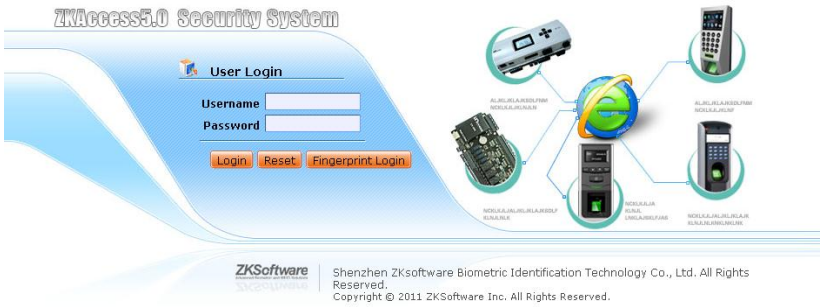
1. Log in to the System

After installing the server on the computer, the user can access the server through the network and use this system.

Open the browser and enter the server's IP address in the address bar. Press [Enter] to access the system homepage.

If you use the program at the server computer, open [Server Controller] first, and start the service. Then double click the **[ZKAccess Security System]** shortcut on the desktop, following the homepage pops up.

Note: Right click [Server Controller] and select [Run as Administrator] in Windows 7/Vista system.



For system security, it is required to verify identity before accessing the system. We will provide a super user (having all operation levels) to begin the system. Enter user name and password, and click [login], or click [Fingerprint Login], and then press the administrator fingerprint on the fingerprint sensor (need to install the fingerprint sensor driver first) to enter the system.

Note: The user name of the super user is [admin], and the password is [admin]. After the first login to the system, for system security, please use the [Modify password] function to modify the password.

The super user can assign company personnel as system users to (such as management personnel, registrar, and access control administrator) and configure the roles of corresponding modules. For details, see 7.1 User Management.

2. Quit the System:

Click the [Logout] button in the upper right corner of the interface to return to the ZKAccess 5.0 homepage.

Or close the browser directly to quit the system.

After that, enter the [Server Controller] and stop the server, then quit the [Server Controller].

3. Customize Settings:

The user can use this function to customize the main interface. Click [Setting] to activate the Setting interface and enter the following information: E-mail Address, First Name, Last Name and Language. Click [Confirm] to complete setting.

The modified system interface will change accordingly, such as the desired language.

4. System User Manual:

Press the help icon to view the system help file. On each operation interface, a "(?)" icon will appear on the right top of the interface, indicating the help for the current page. Click it to view the help file.

5. Modify Password:

The super user and the new user created by the super user (the default password for the new user is "111111") can use the [Modify Password] function to modify the login password for system security. Click [Modify Password], it pops up the Edit Page.

Enter the old password and the new password, confirm the new password and click [Confirm] to complete the modification.

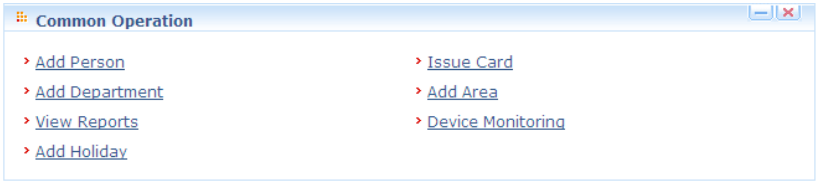
Note: The user name is case-insensitive, but the password is case-sensitive.

3. My Work Panel

After the user logs in to the system it will show the [My Panel] main interface, displaying common operations and other important information.

The default work panel includes the following modules:

❁ **Common Operation:** The user can rapidly perform some common operations here, as shown below.



Add Person please refer to 4.2.1 Add Personnel;

Card Issue please refer to 4.2.2 Personnel Information Maintenance;

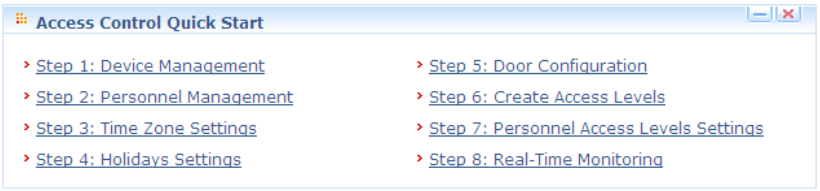
Add Department please refer to 4.1 Department Management;

Add Area please refer to 5.1 Area Settings;

View Reports please refer to 6.7 Access Control Reports;

Device Monitoring please refer to 5.3 Device Communication Management;

❁ **Access Control Quick Start:** Follow the steps to enter corresponding modules for related operations, fulfilling access control functions.


Access Control Quick Start
Step 1: Device Management
Step 2: Personnel Management
Step 3: Time Zone Settings
Step 4: Holidays Settings
Step 5: Door Configuration
Step 6: Create Access Levels
Step 7: Personnel Access Levels Settings
Step 8: Real-Time Monitoring

Device Management please refer to 5.2 Device Management;

Personnel Management please refer to 4.2 Personnel Management;

Time Zone Settings please refer to 6.1 Access Control Time Zones;

Holidays Settings please refer to 6.2 Access Control Holidays;

Door Configuration please refer to 6.3 Door Settings;

Create Access Levels please refer to 6.4 Access Levels;

Personnel Access Levels Settings please refer to 6.5 Personnel Access Levels;

Real-time Monitoring please refer to 6.6 Real-time Monitoring;

Customize Work Panel:

Click [Customize Work Panel] in the upper right corner to open a dialog box. Cancel the tick of the undesired modules (all ticked by default) and click [OK] to complete the setting. Now customized modules are displayed;

Or, directly click the "—" icon on a module to minimize, and click the "✕" icon to close the module. Click the upper bar to drag and adjust its position;

To restore the original panel, click [Restore Work Panel] to refresh and return to the system default work panel.

4. Personnel System Management

Before using the system's access control management functions, access the personnel system to configure: First, Department Management settings used to set the company's organizational chart; Second, Personnel Management settings used to input personnel, assign departments, and maintain and manage personnel. Then set Access Control.

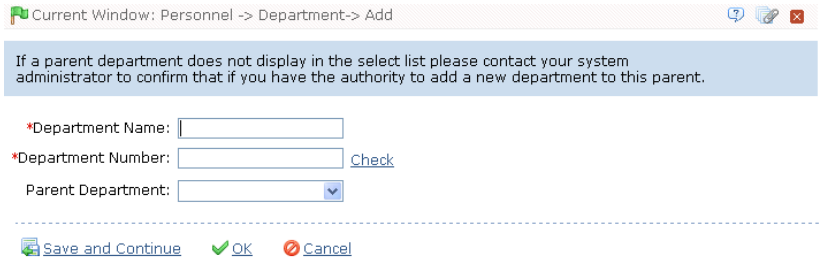
4.1 Department Management

Before managing company personnel, it is required to describe and manage the company's departmental organization chart. Upon first use of the system, by default it has a primary department named **[Company Name]** and numbered **[1]**. This department can be modified but cannot be deleted.

Main functions of Department Management include Add Department and Department Maintenance.

1. Add Department:

Click [Personnel] - [Department] - [Add] to show the Add Department edit interface.


Current Window: Personnel -> Department-> Add
If a parent department does not display in the select list please contact your system administrator to confirm that if you have the authority to add a new department to this parent.
*Department Name:
*Department Number:
Check
Parent Department:
Save and Continue
OK
Cancel

The fields are as follows:

Department Name: Any character, up to a combination of 100 characters;

Department Number: If required, it cannot be identical to another department. The length cannot exceed 100 digits. Click [Verify] to see if it is a duplicate or not;

Parent Department: Select from the pull-down menu and click [OK];

After editing, click [OK] to complete adding, or click [Cancel] to cancel it.

To add a department, you can also use [Import] to import department information from other software or another document into this system. For details, see Appendix 1 Common Operation. [Upper Department] is an important parameter to determine the company's organizational chart. On the right of the interface, the company's organizational chart will be shown in the form of a department tree.

2. Department Maintenance:

Department Maintenance includes department Edit and Delete:

Upon a change to the department or organizational structure, the user can use the [Edit] function to modify such items as Department Name, Department Number or Upper Department. Click Department Name directly or click the [Edit] button behind the department to access the edit interface for modification.

To delete a department, click the check box before the department, and click [Cancel Department], or directly click the [Delete] button behind the department.

Note: A department cannot be deleted freely. If so, the personnel under the department will be pending, and some historical data will not be able to be queried. If deletion is required, please first transfer the departmental personnel to another department.

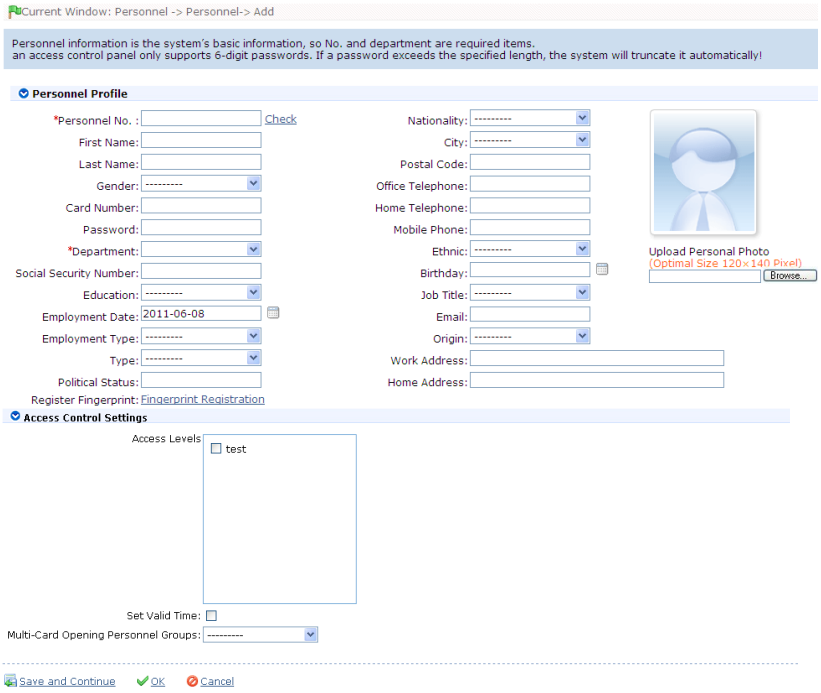
4.2 Personnel Management

When starting to use this management program, the user must register personnel in the system, or import personnel

information from other software or another document into this system. For details, see Appendix 1 Common Operation.

4.2.1 Add Personnel

Click [Personnel] - [Personnel] - [Add] to show the Personnel Profile edit interface:



The fields are as follows:

Personnel No.: By default, the length cannot exceed 9 digits. A number with a length of less than 9 digits will be preceded with 0 automatically to complete 9 digits. Numbers cannot be duplicated. Click [Verify] to see if it is duplicated or not;

Department: Select from the pull-down menu and click [OK]. If the department was not set previously, you can only select the default [Company Name] department;

Social Security Number: Duplication is not allowed. Click [Verify] to check duplication. 15-digit and 18-digit ID card numbers are supported;

Card Number: Assign a card number to the person for access control use. This can be done manually or by using a card issuer. For details, see Personnel Card Issue in 4.2.2 Personnel Information Maintenance;

Password: Set personnel password. An access control panel only supports 6-digit passwords. If a password exceeds the specified length, the system will truncate it automatically. If you need to modify the password, please clear the old password in the box and input the new one;

Personal Photo: The best size is 120×140 pixels for saving space. For details, see Upload Personal Photo in 4.2.2 Personnel Information Maintenance;

Employment Date: By default it is the current date.

Register Fingerprint: Enroll the Personnel Fingerprint or Duress Fingerprint. If the person presses the Duress Fingerprint, it will trigger the alarm and send the signal to the system.

Note: If you have not installed the fingerprint sensor driver, the system will prompt to download and install the driver when you click “Register Fingerprint” (Fingerprint function is only available for version 5.0.8 and above).

Access Control Settings: Select access levels, start and end dates of access validity time and multi-card opening personnel groups (Presetting is required. For details, see 6.3.3 Multi-Card Opening);

Validity time is set for temporary access control, where the door can be opened only during this time period. If not ticked, the

setting will be always valid.

After editing personnel information, click [OK] to save and quit. The added personnel will be shown in the personnel list.

Note: The number of a person, whether departed or in service, must be unique. The system, when verifying, will automatically search the number in the departure library.

The Personnel Information List, by default, is displayed as a table. If Graphic Display is selected, photos and numbers will be shown. Put the cursor on a photo, details about the person will be shown.

4.2.2 Personnel Information Maintenance

The operations include Personnel Card Issue, Upload Personal Photo, etc.

For such functions, you can directly click the personnel number in the personnel list to enter the edit interface for modification, or click the [Edit] button under “Related Operation” to enter the edit interface for modification. After modification, click [OK] to save and quit.

1. Personnel Card Issue:

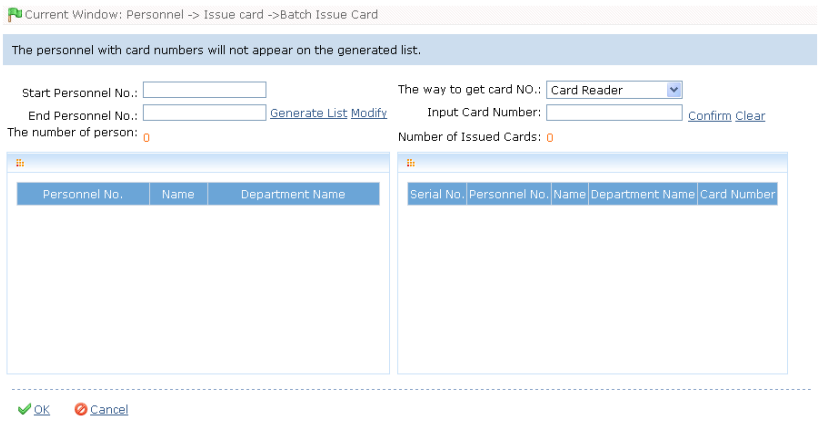
Assign card numbers to personnel, including batch card issue and individual card issue.

(1) How to use the Card Issuer:

The card issuer is connected to the PC through a USB port. When the cursor is on the Card Number Input box, punch the card on the card issuer, then the card number will display in the input box.

(2) Batch Card Issue:

Click [Personnel] - [Issue Card] - [Batch Issue Card] to show the Batch Issue Card edit interface;



Enter Start and End Personnel Numbers (not longer than the system support max digits) to generate personnel list and show all personnel without cards within this number series;

Select [The way to get card NO.]: Card Reader or Access Control Panel.

When using the card reader, swipe the card near the card reader. The system will get the card number and issue it to the user in the left list.

Using the access control panel, select the position of swiping card, such as a card reader connected to an access control panel. Click [Start to read], the system will read the card number automatically, and issue it to the user in the left list one by one. After that, click [Stop to read].

Click [OK] to complete card issue and return. Personnel and corresponding card numbers will be shown in the list.

(3) Individual Card Issue:

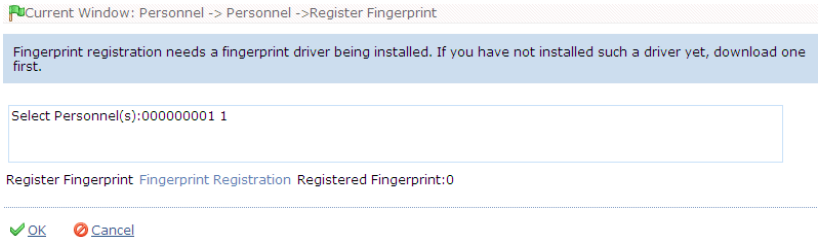
Click [Personnel] - [Card Issue] - [Add] to show Individual Card Issue interface;

Select personnel, enter card number (or use card issuer for card issue), select card issue date, and click [OK].

Note: A person can be issued cards only once. Card modification can only be completed by editing personnel information. The system supports card issue through card issuer and by manually inputting card numbers.

2. Register Fingerprint

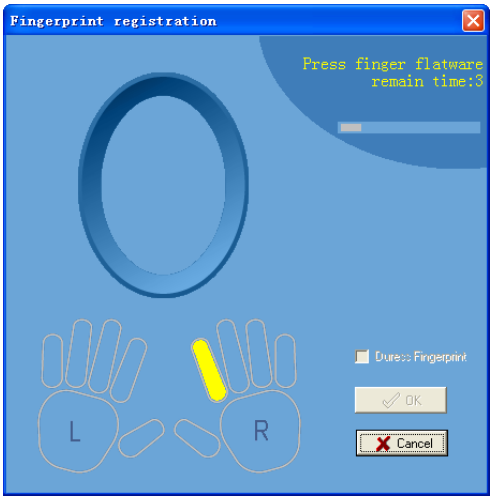
(1) Click [Personnel] - [Personnel], select personnel, and click [Register Fingerprint] to open the Fingerprint Registration edit interface:


Current Window: Personnel -> Personnel ->Register Fingerprint
Fingerprint registration needs a fingerprint driver being installed. If you have not installed such a driver yet, download one first.
Select Personnel(s):000000001 1
Register Fingerprint Fingerprint Registration Registered Fingerprint:0
OK
Cancel

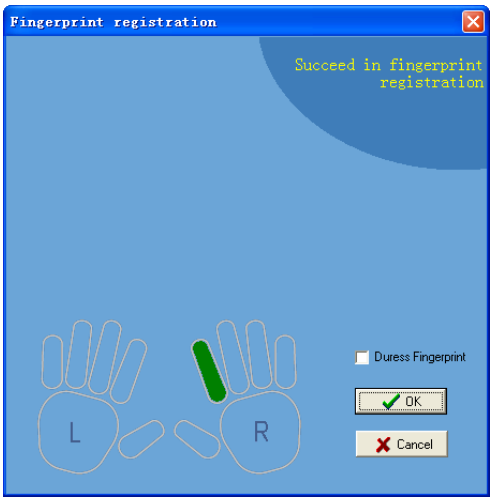
If you have enrolled fingerprints, the number of enrolled fingerprints will show after corresponding item.

(2) Click [Fingerprint Registration] to open the Fingerprint Registration interface.

Note: If there is no fingerprint driver installed, the system will prompt to download and install the driver.



(3) Click the finger for the fingerprint to be enrolled. After the finger finishes 3 times press the FP Sensor. The system prompt “Succeed in fingerprint registration” is shown, as blow:



(4) The enrolled fingerprint will be indicated in this diagram. Click [OK] to save and close the current interface and return to the previous window.

To delete the fingerprints, please click on the enrolled finger twice. The system prompts confirmation for the deletion.

If you want to enroll a Duress Fingerprint, tick the Duress Fingerprint option before enrolling.

3. Upload Personal Photo:

Click [Personnel] - [Personnel], tick the personnel (only one person can be selected), click [Upload Personal Photo], enter the edit interface, click [Browse], select a photo, and click [OK] to save and exit.

4.2.3 Personnel Adjustment

Personnel Adjustment is daily maintenance of existing personnel, primarily including: Personnel Adjust Department and Delete Personnel.

1. Personnel Adjust Department:

Operation steps are as follows:

(1) Click [Personnel] - [Personnel], and select the person subject to department adjustment from the personnel list. Click the [Adjust Department] button, and the following interface appears;

(2) Select the department to be transferred to.

(3) After editing, click [OK] to save and quit.

2. Delete Personnel:

Click [Personnel] - [Personnel], select personnel, click [Delete], and click [OK] to delete, or directly click [Delete] under “Related Operation” of the personnel to delete.

Note: Deleting personnel also results in deleting the personnel in the database.

5. Device Management

The access control panel to be connected to this system provides access control system functions. To use these functions, the user must first install devices and connect them to the network. Second, set corresponding parameters in the system so as to manage these devices via the system, upload user access control data, download configuration information, output reports and achieve digital management of the enterprise.

Device Management primarily includes Area Setting, Device Management, and Device Monitoring.

5.1 Area Settings

Area is a spatial concept, enabling the user to manage devices in a specific area.

In the access system, after area setting, device (doors) can be filtered by area upon real-time monitoring.

The system, by default, has set an area named [Headquarters] and numbered [1]. Area Setting includes Add Area and Delete Area.

1. Add Area:

Click [Device] - [Area Settings] - [Add] to activate the Add Area edit interface;

The fields are as follows:

Area Number: Repetition not allowed;

Area Name: Any character up to a combination of 30 characters;

Parent Area: Decides the regional organization structure of the company.

After setting, click [OK].

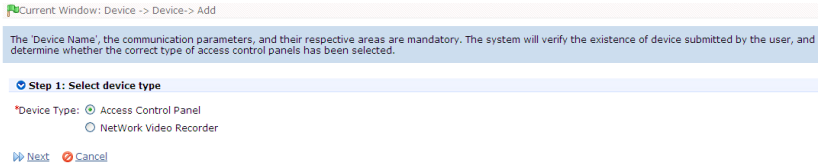
2. Delete Area:

Select area, click [Delete Area], or directly click [Delete Area] under “Related Operation” of an area, and click [OK].

5.2 Device Management

Set the communication parameters of connected devices. Only when communication parameters, including system settings and device settings are correct, normal communication with devices will be possible. When communication is successful, you can view the information of connected devices and perform remote monitoring, uploading and downloading data.

It includes Add Access Control Panel and Add Network Video Recorder. Click [Device] - [Device] - [Add], the system will prompt to select the device type.


Current Window: Device -> Device-> Add
The 'Device Name', the communication parameters, and their respective areas are mandatory. The system will verify the existence of device submitted by the user, and determine whether the correct type of access control panels has been selected.
Step 1: Select device type
*Device Type:
Access Control Panel
NetWork Video Recorder
Next
Cancel

To add Access Control Panel, search and view devices connected to the network, and directly add from the search result.

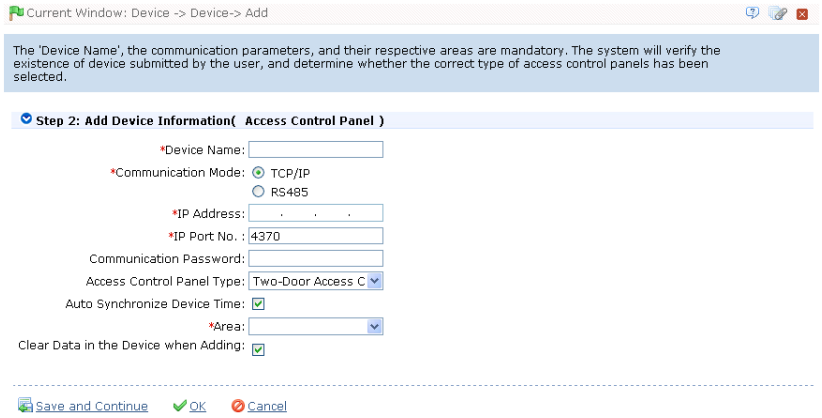
5.2.1 Add Access Control Panel

There are two ways to add Access Control Panel.

1. Add Device:

(1) In the Device Type Selection interface, select Add Access Control Panel. The communication modes are TCP/ IP or RS485. The following interface will be shown:

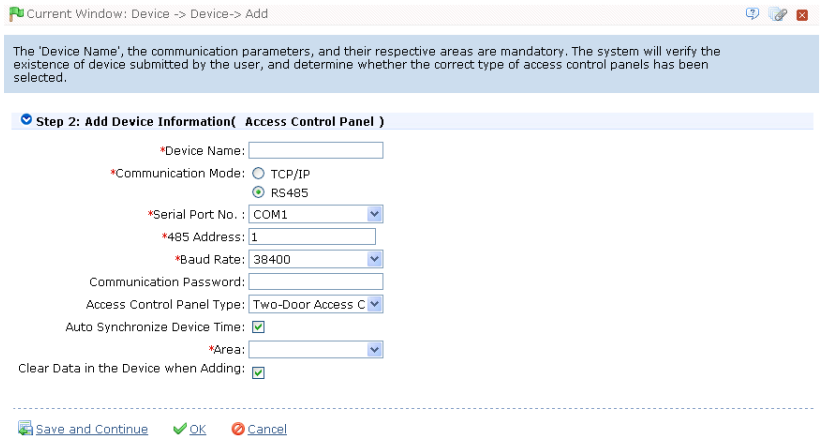
TCP/ IP:


Current Window: Device -> Device-> Add
The 'Device Name', the communication parameters, and their respective areas are mandatory. The system will verify the existence of device submitted by the user, and determine whether the correct type of access control panels has been selected.
Step 2: Add Device Information(Access Control Panel)
*Device Name:
*Communication Mode: TCP/IP
RS485
*IP Address:
*IP Port No. : 4370
Communication Password:
Access Control Panel Type: Two-Door Access C
Auto Synchronize Device Time:
*Area:
Clear Data in the Device when Adding:
Save and Continue
OK
Cancel

IP Address: Please enter the IP Address of the access control panel;

IP Port No.: In Ethernet mode, the default is 4370;

RS485:


Current Window: Device -> Device-> Add
The 'Device Name', the communication parameters, and their respective areas are mandatory. The system will verify the existence of device submitted by the user, and determine whether the correct type of access control panels has been selected.
Step 2: Add Device Information(Access Control Panel)
*Device Name:
*Communication Mode: TCP/IP
RS485
*Serial Port No. : COM1
*485 Address: 1
*Baud Rate: 38400
Communication Password:
Access Control Panel Type: Two-Door Access C
Auto Synchronize Device Time:
*Area:
Clear Data in the Device when Adding:
Save and Continue
OK
Cancel

Serial Port Number: COM1-COM254;

485 Address: The machine number. When serial port numbers are the same, there will be no repeated 485 addresses;

Baud Rate: Same as the baud rate of the device (9600/ 19200/ 38400/ 57600/115200). The default is 38400;

Device Name: Any character, up to a combination of 20 characters;

Communication Password: Any character, up to a combination of 15 characters (No blank). You need to input this field only when you add a new device with the communication password. It cannot be modified when you edit the device information except in [Modify Communication Password] operation. Please refer to 6.3.1 Door Management.

Note: You do not need to input this field if the device has no communication password, such as when it is a new factory device or just after initialization.

Panel Type: One-door panel, two-door panel, four-door panel;

Switch to Two-door Two-way: When four-door panel is selected, this box will appear. By default, it is not ticked. This parameter is used to switch the four-door one-way access control panel to two-door two-way access control panel (For changes of extended device parameters before and after switching, see relevant files of access control panel).

Note: After the four door one-way access control panel is switched to two- door two-way access control panel, to switch back, you need delete the device from the system and add it again. When adding, do not tick the check box before this parameter.

Auto Synchronizes Device Time: By default it is ticked, namely, it will synchronize device time with server time each time

connecting to the device. If it is not ticked, the user can manually synchronize device time;

Area: Specify areas of devices. After Area Setting, devices (doors) can be filtered by area upon Real-time Monitoring.

Clear Data in the Device when Adding： If this option is ticked, after adding device, the system will clear all data in the device, except the event logs. If you add the device just for demonstration or testing of the system, there is no need to tick it.

(2) After editing, click [OK] and the system will try connecting the current device:

If connection is successful, it will read the corresponding extended parameters of the device. At this time, if the access control panel type selected by the user does not meet the corresponding parameters of the actual device, the system will remind the user. If the user clicks [OK] to save, it will save the actual access control panel type of the device.

Extended Device Parameters: includes serial number, device type, firmware version number, auxiliary input quantity, auxiliary output quantity, door quantity, device fingerprint version, and reader quantity.

If device connection fails while the user still needs to add the device to the system, corresponding device parameters and extended parameters such as the serial number, will not be written into the system and settings such as anti-pass back and linkage will not be possible. These settings can be created only when the device is reconnected successfully and corresponding parameters are acquired.

Note: When you add a new device to the system, the software will clear all user information, time zones, holidays, and access control levels settings (including access control group, anti-pass back, interlock settings, linkage settings, etc.) from the device, except the events record in the device. Unless the information in the device is unusable, we recommend that you not delete the device to avoid the loss of information.

Access Control Panel Settings:

❁ TCP/ IP Communication Requirements:

To support and enable TCP/ IP communication, directly connect the device to the PC or connect to the Internet, get the device IP address and other device information;

❁ RS485 Communication Requirements:

To support and enable RS485 communication, connect to the PC through RS485, get the serial port number, RS485 machine number (address), baud rate and other device information.

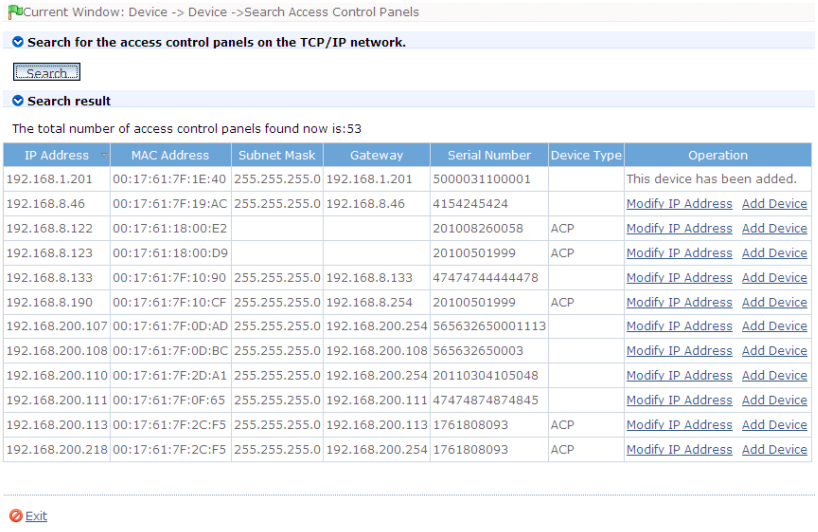
2. Add Device by Searching Access Control Panels:

Search the access control panels in the Ethernet.

(1) Click [Device] - [Device] - [Search Panels], to show the Search interface;

(2) Click [Start Search], and it will prompt [searching……];

(3) After searching, the list and total number of access control panels will be displayed;



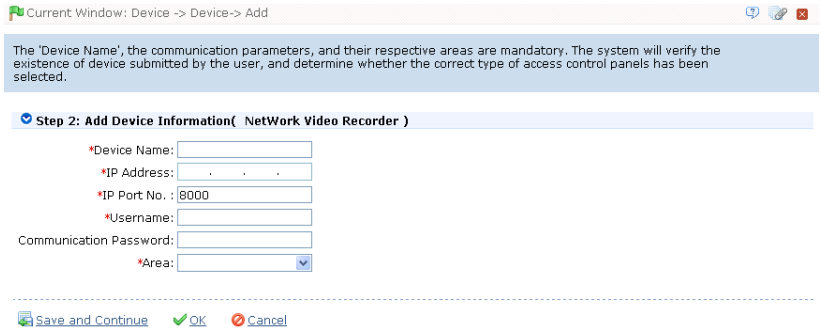
Note: Here we use UDP broadcast mode to search the access controller. This mode cannot exceed the HUB scale. The IP address can exceed the net segment, but must belong to the same subnet and needs to configure the gateway and IP address in the same network segment.

(4) Click [Add to Device List] behind the device, and a dialog box will open. Enter self-defined device name, and click [OK] to complete device addition.

(5) The default IP address of the access control panel may conflict with the IP of a device on the Internet. You can modify its IP address: Click [Modify IP Address] behind the device and a dialog box will open. Enter the new IP address and other parameters (Note: Must configure the gateway and IP address in the same network segment);

5.2.2 Add Network Video Recorder (For Professional Version 5.0.8 and above)

(1) In Device Type Selection interface, select Add Network Video Recorder. The following interface appears. Click [Next] and set the server information.


Current Window: Device -> Device-> Add
The 'Device Name', the communication parameters, and their respective areas are mandatory. The system will verify the existence of device submitted by the user, and determine whether the correct type of access control panels has been selected.
Step 2: Add Device Information(NetWork Video Recorder)
*Device Name:
*IP Address:
*IP Port No. : 8000
*Username:
Communication Password:
*Area:
Save and Continue
OK
Cancel

IP Address: The IP address of the device.

IP Port: IP port of the device, 8000 by default.

User Name: The user name to login to the device.

Communication Password: The password to login the device.

(2) After edition, click [OK] and the new video server will display on the device list. Currently, the system only supports Hikvision Network Video Recorder.

5.2.3 Device Maintenance

Synchronize All Data: The system will synchronize the data to the device, including door information, access control levels (personnel information, access control time zones), anti-pass back settings, interlock settings, linkage settings, first-card normal open settings, multi-card normal open settings, etc. Select device, click [Synchronize All Data] and click [OK] to complete synchronization.

Note: The operation of Synchronize All Data is mainly to delete all data in the device (except event record). Download all settings again. Please keep the net connection stable and avoid power down situations, etc. If the device is working normally, use this function with caution. Execute it in rare user situations to avoid impact on normal use of the device.

Delete: Select device, click [Delete], and click [OK].

Edit: Click device name, or click [Edit] under “Related Operation” behind the device to open the edit interface.

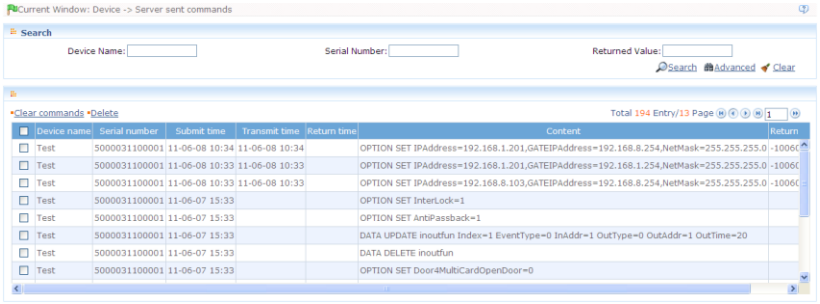
For the meanings and settings of the parameters, see the relevant chapters for details. The gray items are not editable. The device name cannot be identical to the name of another device.

Since the device type cannot be modified, if the type is wrong, the user must manually delete the device and add it again.

5.3 Device Communication Management

1. Commands Sent by Server

Shows the list of commands sent to the device by the current system. If the return value is ≥ 0, execution is successful. If it is a negative, the execution failed.

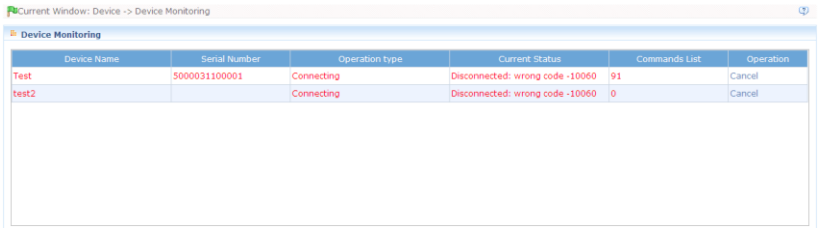

Current Window: Device -> Server sent commands
Search
Device Name:
Serial Number:
Returned Value:
Search
Advanced
Clear
Clear commands
Delete
Total 194 Entry/13 Page
Device name
Serial number
Submit time
Transmit time
Return time
Content
Return
Test 5000031100001 11-06-08 10:34 11-06-08 10:34 OPTION SET IPAddress=192.168.1.201,GATEIPAddress=192.168.8.254,NetMask=255.255.255.0
Test 5000031100001 11-06-08 10:33 11-06-08 10:33 OPTION SET IPAddress=192.168.1.201,GATEIPAddress=192.168.1.254,NetMask=255.255.255.0
Test 5000031100001 11-06-08 10:33 11-06-08 10:33 OPTION SET IPAddress=192.168.8.103,GATEIPAddress=192.168.8.254,NetMask=255.255.255.0
Test 5000031100001 11-06-07 15:33 OPTION SET InterLock=1
Test 5000031100001 11-06-07 15:33 OPTION SET AntiPassback=1
Test 5000031100001 11-06-07 15:33 DATA UPDATE inoutfun Index=1 EventType=0 InAddr=1 OutType=0 OutAddr=1 OutTime=20
Test 5000031100001 11-06-07 15:33 DATA DELETE inoutfun
Test 5000031100001 11-06-07 15:33 OPTION SET Door4MultiCardOpenDoor=0

Clear Command List: Click it to open the Confirm interface. Click [OK] to clear all items in the list of commands sent by the server;

Delete: Tick the check box before the command to be deleted and click [Delete]. Confirm to delete the command.

2. Device Monitoring

By default it monitors all devices with the current user's level, and lists the operation information of the devices: device name, serial number, operation type, current status, commands to be executed, and progress, etc.

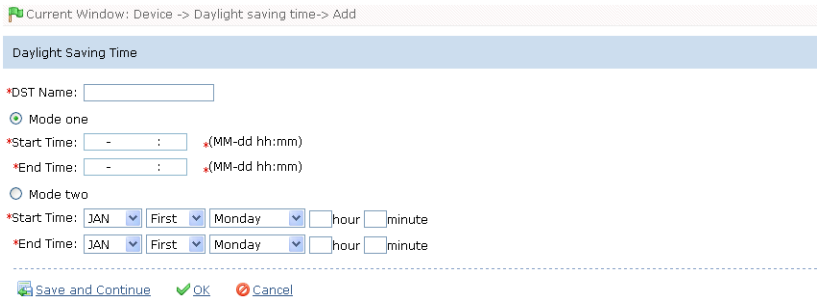


5.4 Daylight Saving Time

DST, also called Daylight Saving Time, is a system that prescribes the local time setting principle in order to save energy. The unified time adopted during the system date is called "DST". Usually, the time will be one hour forward in summer. It encourages people to go to bed early and wake up early in order to reduce lighting and save energy. In autumn, the time will be recovered. The regulations are different in different countries.

To meet the demand of DST, a special option can be customized on this system. Set the time one hour forward at XX (minute) XX (hour) XX (day) XX (month), and set the time one hour backward at XX (minute) XX (hour) XX (day) XX (month) if necessary.

Note: If a DST setting is in use, it cannot be deleted. First stop the DST then delete it again.


Current Window: Device -> Daylight saving time-> Add
Daylight Saving Time
*DST Name:
Mode one
*Start Time: - : *(MM-dd hh:mm)
*End Time: - : *(MM-dd hh:mm)
Mode two
*Start Time: JAN First Monday hour minute
*End Time: JAN First Monday hour minute
Save and Continue
OK
Cancel

1. DST Adding:

Mode 1: Set as "Month-day hour: minute" format, Start Time and End Time is needed. For example, the Start Time can be set as "3-11 00:00", when the start time arrives, the system will be advanced one hour. When the end time arrives, the system will

turn back to the original time.

Mode 2: Set as "Month-Weeks-week hour: minute" format. The start time and end time is needed. For example, the start time can be set “second Monday in March, 00:00” When the start time arrives, the system will be advanced one hour. When the end time arrives, the system will turn back to the original time.

2. DST Using:

The user can enable the DST setting on a device in the following ways:

In the DST interface, select a DST setting, and click [Daylight Saving Time setting], select the device to apply the DST setting to and click [OK] to confirm.

Otherwise, in the [Access Control] – [Door Configuration] interface, select the device, and click [Enable Daylight Saving Time] or [Disable Daylight Saving Time] to set.

If a DST setting is in use, the latest modification will be sent to the device. The device disconnect will lead to transmission failure, and it will continue transmit at the next connection.

In the Door Management module of the access control system, you can enable or disable the DST function. If you enable the DST setting, when the start time arrives, the system will be advanced one hour. When the end time arrives, the system will turn back to the original time. If you have not set a DST in the device, when you disable DST, the system will prompt “The Daylight Saving Time hasn’t been set in this device”.

6. Security System Management

1. Work principle of the access control system:

ZKAccess5.0 Security System is a WEB-based management system, providing normal access control functions, management of networked access control panel via computer, and unified personnel access management.

The access control system can set the opening levels of registered users, namely, allowing some personnel to open some doors by verification during a time period.

Otherwise, the system supports the use of data from the access control panel for attendance purpose, to save the device resource.

It facilitates the management and support of multiple databases, including MySQL, SQL Server, and Oracle. Designed based on multi-business convergence, it supports service extension, such as attendance, patrol, visitor management, etc., and supports multiple languages.

2. Access control system parameters:

- 256 time zones;
- 256 access levels;
- Three holiday types and 96 holidays total;
- Anti-pass Back function;
- Interlock function;
- Linkage function;
- First-Card Normal Open function;
- Multi-Card Opening function;
- Remote door opening and closing;
- Real-time monitoring via Web browser;

3. Operation functions of access control system:

Click to enter the [Access Control System] and the main interface is [Real-time Monitoring].

Access Control System Management primarily includes Access Control Time Zones, Access Control Holiday, Door Settings, Access Levels, Personnel Access Levels, Real-time Monitoring, Reports, etc.

6.1 Access Control Time Zones

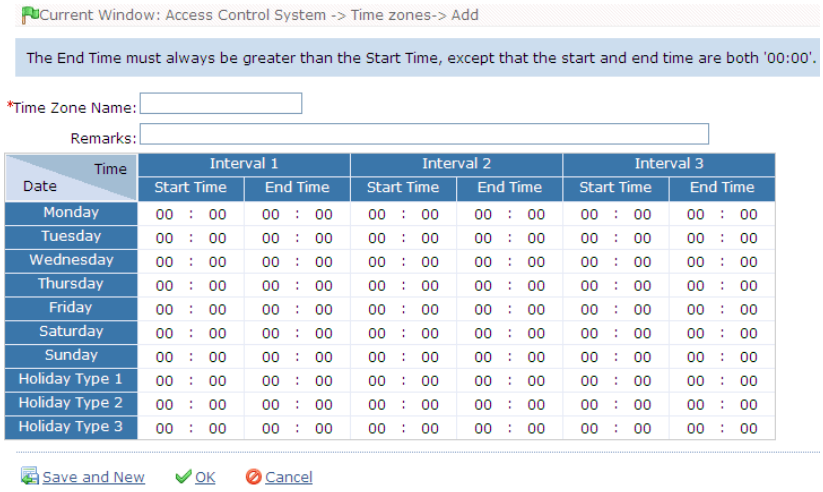
Access Control Time Zone can be used for door timing. The reader can be made usable during valid time periods of certain doors and unusable during other time periods. Time Zone can also be used to set Normal Open time periods for doors or set access control levels so that specified users can only access specified doors during specified time periods (including access levels and First-Card Normal Open settings).

The system controls access according to Access Control Time Zones. The system can define up to 255 time zones. During a week, you can define up to three intervals for each day and three holiday types for each time zone. Each interval is the valid interval in the 24 hours of each day. The format of each interval for a time zone is: HH: MM-HH: MM, this is accurate to minutes in the 24-hour system.

Initially, by default the system has access control time zone named [Accessible 24 hours]. This time period can be modified but cannot be deleted. The user can add Access Control Time Zones that can be modified.

1. Add Access Control Time Zone:

(1) Click [Access Control System] - [Time zones] - [Add] to access the Time Zone setting interface;



The parameters are as follows:

Time Zone Name: Any character, up to a combination of 30 characters;

Remarks: Detailed description of the current time zone, including an explanation of the current time zone and primary applications facilitating the user or other users with same level to view time zone information. The field is up to 70 characters;

Interval and Start/End time: One Access Control Time Zone includes 3 intervals for each day in a week, and three intervals for each of the three Access Control Holidays. Set the Start and End Time of each interval;

Setting: If the interval is Normal Open, just enter 00:00-23:59 as the first interval, and 00:00-00:00 as the second and third intervals. If the interval is Normal Close, all are 00:00-00:00. If only using one interval, the user just need to fill out the first interval (such as: Normal Open) and the second and third intervals will use the default value of 00:00-00:00. Similarly, when the user only uses the first two intervals, the third interval will use the default value of 00:00-00:00. When using two or three intervals, the user needs to ensure two or three intervals have no time intersection and the time does not span days. Otherwise, the system will prompt error.

Holiday Type: There are three holiday types in the time zone. They are unrelated to the day of the week. If a certain date is set to a certain holiday type, the three intervals of the holiday type will be used for access. The holiday type in a time zone is optional. However, if the user does not enter one, the system will give the default value.

For example, set the access control interval of Holiday Type 1 as 8-20, the Access Control Time Period of Holiday Type 2 as Normal Open, and the Access Control Time Zone of Holiday Type 3 as Normal Close.

(2) After time zone setting, click [OK] to save and the time zone will appear in the list.

2. Maintenance of Access Control Time Zone:

Edit: In the time zone list, click the [Edit] button under “Related Operation” to access the time zone modification interface and modify the time zone setting. After modification, click [OK] and the modified time zone will be saved and shown in the time zone list.

Delete: In the time zone list, click the [Delete] button under “Related Operation”. Click [OK] to delete the time zone or click [Cancel] to cancel the operation. A time zone in use cannot be deleted.

Tick the check boxes before one or more time zones in the time zone list. Click the [Delete] button over the list, and click [OK] to delete the selected time zones, or click [Cancel] to cancel the operation.

6.2 Access Control Holidays

The Access Control Time of a holiday may differ from that of a weekday. For easy operation, the system provides holiday settings to set access control time for holidays.

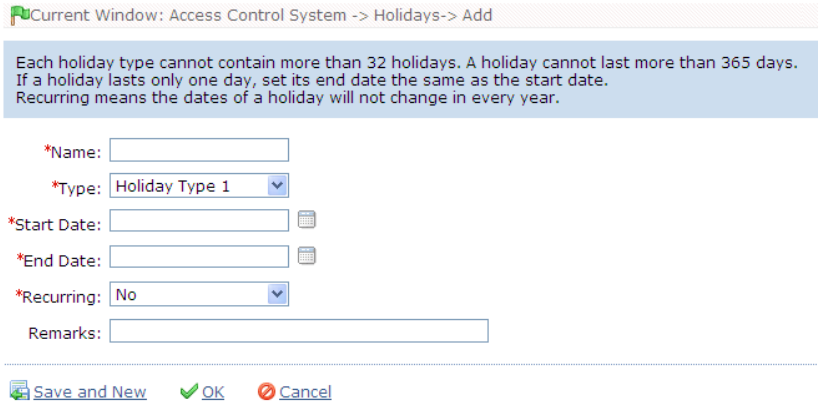
Access Control Holiday Management includes Add, Modify and Delete Access Control Holiday.

1. Add Access Control Holiday:

Three holiday types are supported, each including up to 32 holidays. To conduct special access level configuration on special dates, the user can select special holidays for setting.

The operation steps are as follows:

(1) Click [Access Control System] - [Holidays] - [Add] to access Add Access Control Holiday edit interface:


Current Window: Access Control System -> Holidays-> Add
Each holiday type cannot contain more than 32 holidays. A holiday cannot last more than 365 days.
If a holiday lasts only one day, set its end date the same as the start date.
Recurring means the dates of a holiday will not change in every year.
*Name:
*Type:
Holiday Type 1
*Start Date:
*End Date:
*Recurring:
No
Remarks:
Save and New
OK
Cancel

The fields are as follows:

Holiday Name: Any character up to a combination of 30 characters;

Holiday Type: Holiday Type 1/2/3. A current holiday record belongs to these three holiday types and each holiday type includes up to 32 holidays;

Start/ End Date: Must meet the date format as “2010-1-1”. The Start Date cannot be later than the End Date otherwise the system will prompt an error. The year of the Start Date cannot be earlier than the current year and the holiday cannot span years;

Recurring: Yes or No. The default is “No”. Annual cycle means that a holiday does not require modification in different years. For example, the Near Year’s Day is on January 1 each year and can be set as “Yes”. For another example, Mother's Day is on the second Sunday of each May, so its date is not fixed and should be set as “No”.

For example, the date of the holiday “New Year’s Day” is set as January 1, 2010, and the holiday type is 1, then on January 1, Access Time Control will not follow the time of “Friday” in the week, but the Access Control Time of Holiday Type 1.

(2) After editing, click the [OK] button to save and it will appear in the holiday list.

2. Modification of Access Control Holiday:

To modify the original Access Control Holiday, click [Edit] behind the Access Control Holiday to access the edit interface. After modification, click [OK] to save and quit.

3. Deletion of Access Control Holiday:

In the access control holiday list, click the [Delete] button under “Related Operation”. Click [OK] to delete the holiday, or click [Cancel] to cancel the operation. An Access Control Holiday in use cannot be deleted.

Tick the check boxes before one or more holidays in the holiday list. Click the [Delete] button over the list, and click [OK] to delete the selected holiday, or click [Cancel] to cancel the operation.

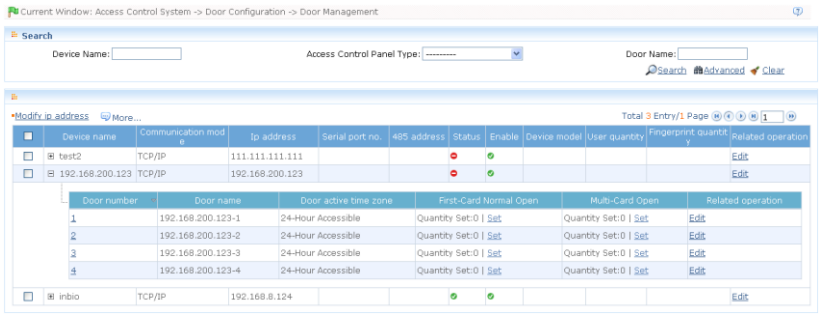
6.3 Door Settings

Currently the system supports the connection and control of up to 50 access control panels.

The access control system is primarily for the management of personnel restriction and admission. For security, a company will set personnel admission time zones, restricted time zones and combinations of time zones. For door opening verification, First-Card Normal Open, Multi-Card Opening, anti-pass back, linkage, and interlock can be set to enhance security. This system can provide real-time monitoring of doors and output of exception, access control events and access level reports.

6.3.1 Door Management

Click [Access Control System] - [Door Configuration], and by default it will access the [Door Management] interface showing the list of all control panels. When unfolded, it can show all doors under the control of the control panel. Upon first entry into the access interface or successful query, if system the currently has access control panels or the query result is not null, by default it will unfold the doors of the first access control panel. Click the corresponding button for relevant parameter settings.



Door Management operations include: Control Panel Management and Door Management.

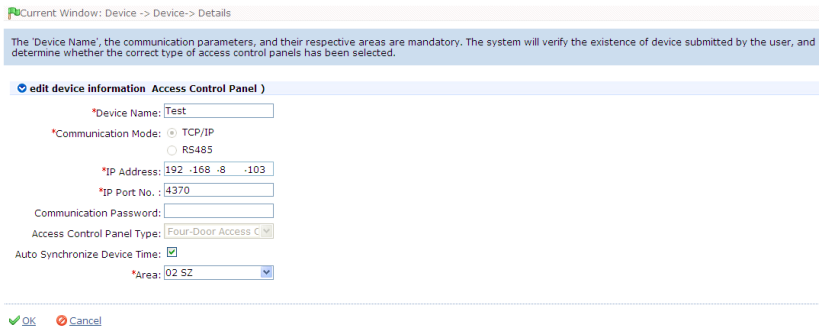
1. Access Control Panel Operation

For communication between the system and the device, data uploading, configuration downloading, device and system parameters shall be set. The user can see access control panels within his level in the current system, and can edit the devices here. The user can to add or delete devices in Device Management if needed.

Control Panel Management includes: Modify IP Address, Close Auxiliary Output, Disable, Enable, Modify Communication Password, Synchronize Time, Upload Event Record, Upgrade Firmware, and Get Event Entries.

(1) Device Profile:

Select device, click [Edit] under “Related Operation”. For Related details, see 5.2.2 Device Maintenance.


Current Window: Device -> Device-> Details
The 'Device Name', the communication parameters, and their respective areas are mandatory. The system will verify the existence of device submitted by the user, and determine whether the correct type of access control panels has been selected.
edit device information Access Control Panel)
*Device Name: Test
*Communication Mode: TCP/IP
RS485
*IP Address: 192 .168 .8 .103
*IP Port No. : 4370
Communication Password:
Access Control Panel Type: Four-Door Access C
Auto Synchronize Device Time:
*Area: 02 SZ
OK
Cancel

(2) Modify IP Address:

Select device and click [Modify IP Address] to show the Modification interface. It will obtain Real-time Network gateway and mask from the device. If it fails because the network is unavailable, then the IP address cannot be modified. Enter new IP address, gateway, and subnet mask. Click [OK] to save settings and quit. This function is the same as [Modify IP Address Function] in 5.2.1 Add Access Control Panel. The difference is when searching control panels, the devices have not been added into the system, while the current [Modify Device IP Address] is regarding added devices.

(3) Disable/Enable:

Select device, click [Disable/Enable] to stop/start using the device. When the device’s communication with the system is interrupted or the device fails, the device may automatically appear in disabled status. At this time, after adjusting Internet or device, click [Enable Device] to reconnect the device and restore device communication.

Note: If the current device is in enabled status and the connection is not successful, if the user performs the enable operation, the system will immediately reconnect the device.

(4) Modify Communication Password:

Enter the old communication password before modification. After verification, input the same new password twice, and click [OK] to modify the communication password.

Note: The communication password cannot contain spaces, it is recommended that a combination of numbers and letters be used. The communication password setting can improve the device security. It is recommended to set communication password for each device.

(5) Synchronize Time:

Synchronize device time with current server time.

(6) Get Event Entries:

Get event records from the device into the system.

Three options are provided for this operation, Get New Entries, Get All Entries, and Get Entries from SD Card.

Get New Entries: The system only gets the new event entries since the last time event entries were collected and records them into the database. Repeated entries will not be rewritten.

Get All Entries: The system will get all of the event entries again. Repeated entries will not be rewritten.

Get Entries from SD Card: The system will get the event entries from the SD card in the device.

When the network status is normal and the communication status between the system and the device is normal, the system will acquire event records in the device in real-time and save them into the system database. However, when the network is interrupted or communication is interrupted for any reason and the event records in the device have not been uploaded into the system in real-time, the operation can be used to manually acquire event records in the device. In addition, the system, by default, will automatically acquire event records in the device at 00:00 each day.

Note: The access controller can restore up to 100 thousand event entries. When the entries exceed this number, the device will automatically delete the oldest stored entries (the default delete number is 10 thousand).

(7) Upgrade Firmware

To upgrade firmware in the device, tick the device for which you want to upgrade the firmware, click [Upgrade firmware], enter edit interface, click [Browse] to select the firmware upgrade file (named emfw.cfg) provided by ZKAccess, and click [OK] to start upgrading.

Note: The user shall not upgrade firmware without authorization. Contact the distributor before upgrading firmware, or upgrade it when instructed by the distributor. Unauthorized upgrading may cause problems that affect normal use.

(8) Change the fingerprint identification threshold (only available for version 5.0.8 and above)

The user can change the fingerprint identification threshold in the device. The scale is 35-70 and 55 by default. In device adding, the system will get the threshold from the device. If the operation succeeds, the user can view the threshold in all of the devices. Batch operation is permitted; the user can change multiple devices concurrently.

(9) Enable Daylight Saving Time

Select the Daylight Saving Time being set, click [Enable Daylight Saving Time] to enable it.

(10) Disable Daylight Saving Time

Disable the Daylight Saving Time in use.

(11) Get Information of Personnel

Renew the current number of personnel and fingerprints in the device. The final value will be displayed on the device list.

(12) Close Auxiliary Output

Close the auxiliary device connected to the device auxiliary output interface.

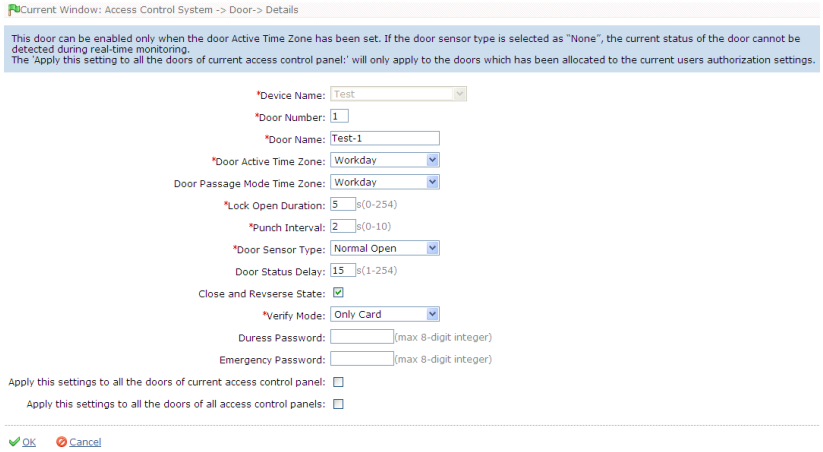
2. Door Management:

The device list will show all access control devices. Click the “+” button before the device name to show the door list under a device. When adding a device, it will automatically add doors (corresponding device name and door numbers cannot be edited)

according to the number of doors. Before using the device (including doors), the user must edit door information one by one (or apply current settings to other doors). After editing, they will be sent to the device, which can be used after successful setting.

(1) Door Parameter Modification:

Select the door to be modified, and click [Edit] under “Related Operation” to show the edit interface;


Current Window: Access Control System -> Door-> Details
This door can be enabled only when the door Active Time Zone has been set. If the door sensor type is selected as "None", the current status of the door cannot be detected during real-time monitoring.
The 'Apply this setting to all the doors of current access control panel:' will only apply to the doors which has been allocated to the current users authorization settings.
*Device Name: Test
*Door Number: 1
*Door Name: Test-1
*Door Active Time Zone: Workday
Door Passage Mode Time Zone: Workday
*Lock Open Duration: 5 s(0-254)
*Punch Interval: 2 s(0-10)
*Door Sensor Type: Normal Open
Door Status Delay: 15 s(1-254)
Close and Revserse State:
*Verify Mode: Only Card
Duress Password: (max 8-digit integer)
Emergency Password: (max 8-digit integer)
Apply this settings to all the doors of current access control panel:
Apply this settings to all the doors of all access control panels:
OK
Cancel

The fields are as follows:

Device Name: It is not editable (must be edited in 5.2.1 Add Access Control Panel);

Door Number: The system automatically names the numbers of doors according to how many doors the device has (for example, the four doors of a four-door control panel are numbered 1, 2, 3 and 4). The number will be consistent with the door number on the device.

Note: By default the number following the underline in the door name is consistent with the door number, but 1/2/3/4 in anti-pass back and interlock refers to the door serial number rather than the number following the door name. They are not necessarily related. The system allows the user to modify the door name so that they are not confused;

Door Name: The default Door Name is “device name_door number”. The field allows the user to modify as required. Up to 30 characters can be entered;

Door Active Time Zone, **Passage Mode Time Zone**: By default both are null. Initialized and added access control time zones will be shown for the user to select. Upon door editing, the door valid time zone is needs to be input. Only after setting the door valid time zone, the door can be opened and closed normally. We recommend to set the door Normal Open time period within the door valid time zone, only in this situation, the door Normal Open time zone is valid;

Note: Consecutive punching of a card having access level of the door 5 times can release the Normal Open status for one day (including First-Card Normal Open), and close the door immediately.

Lock Drive Duration: Used to control the delay for unlocking after card punching. The unit is seconds, and the default is 5 seconds. The user can enter a number between 0-254;

Punch Interval: The unit is seconds (range: 0-10 seconds), and the default is 2 seconds;

Door Sensor Type: NO (door sensor not detected), Normal Open, Normal Close. The default is NO. When editing doors, the user can select the door sensor type to be Normal Open or Normal Close. If Normal Open or Normal Close is selected, it is required to select **door status delay** and whether **close and reverse-lock** is required. By default, once door sensor type is set as Normal Open or Normal Close, the default door status delay will be 15 seconds, and by default it will enable Close and Reverse-lock.

Door Status Delay: The duration for delayed detection of the door sensor after the door is opened. Detection is performed only after the door is opened and the delay duration expired. When the door is not in the “Normal Open” period and the door is opened, the device will start timing. It will trigger an alarm when the delay duration expired, and stop the alarm when you close the door. The default door status delay will be 15 seconds. The **door status delay** should be longer than **Lock Drive Duration**.

Close and Reverse State: Set locking or not after door closing. Tick it for lock after door closing.

Verify Mode: Identification modes include Only Card, Card plus Password, Only Password, Card plus Fingerprint, and Only Fingerprint verify. The default is Only Card or Only Fingerprint. When Card plus Password mode is selected, make sure the door uses a reader with keyboard (the fingerprint verify modes are only available for version 5.0.8 and above);

Duress Password, **Emergency Password**: Upon duress, use Duress Password (used with legal card) to open the door. When opening the door with Duress Password, it will alarm. Upon emergency, the user can use Emergency Password (named Super Password) to open the door. Emergency Password allows normal door opening. Emergency Password is effective in any time zone and any type of verify mode, usually used for the administrator.

Duress Password Opening (used with legal card): When Only Card verify mode is used, you need to press [ESC] first and then press the setting password plus [OK] button. Finally swipe your card. The door opens and triggers the alarm. When Card plus Password verify mode is used, swipe your card first then press the password number plus the [OK] button (same to normal door open in card plus password verify mode). The door opens and triggers the alarm.

Emergency Password Opening: The password must be a number not exceeding 8 digits (integers). The door can be opened just by entering the password. Press [ESC] every time before entering password then press OK to execute.

When using Duress Password or Emergency Password, the interval for entering each number shall not exceed 10 seconds and these two numbers should not be the same.

Apply these settings to all the doors of current access control panel: Click to apply to all doors of the current access control panel;

Apply these settings to all the doors of all access control panels: Click to apply to all doors of all access control panels within the current user's level;

After parameter editing, click [OK] to save and quit.

6.3.2 First-Card Normal Open

First-Card Normal Open: During a specified interval, after the first verification by the person having First-Card Normal Open level, the door will be Normal Open and will automatically restore closing after the valid interval expires.

The user can set First-Card Normal Open for a specific door. The settings include door, door opening time zone and personnel with First-Card Normal Open level. A door can have First-Card Normal Open settings for multiple time zones. The interface of each door will show the number of existing First-Card Normal Open settings. For First-Card Normal Open setting, when adding or editing each record, it is not required to modify the "current door" but is to select time zone. When record adding is successful, add personnel that can open the door for a First-Card Normal Open setting record. On the right of the interface you can browse door opening personnel in a First-Card Normal Open setting and delete current personnel, so that some personnel will not have First-Card Normal Open level any more.

The operation steps are as follows:

1. Click [Set] under "First-Card Normal Open" of a door to show First-Card Normal Open setting interface;

2. Click [Add], select the time zone of First-Card Normal Open, and click [OK] to save the settings;

3. Click [Add an opening person] under "Related Operation" to set personnel having First-Card Normal Open level.

Click [OK] to save and quit editing.

Note: For a door currently in Normal Open time period, consecutive verification of a person having access level for the door for 5 times (the person verification interval should be within 5 second) can release the current Normal Open status and close the door. The sixth person verification will be a normal verification. This function is only effective at the valid door time zone. Normal Open intervals set for other doors within the day and First-Card Normal Open settings will not take effect anymore.

6.3.3 Multi-Card Opening

This function needs to be enabled in some special access occasions where the door will open only after the consecutive verification of multiple people. Any person verifying outside of this combination (even if the person belongs to other combinations) will interrupt the procedure, requiring a 10 second wait to restart verification. It will not open by verification of only one of the combination.

1. Multi-Card Opening Personnel Groups:

It is personnel grouping used to set Multi-Card Opening groups.

(1) Click [Access Control System] - [Door Configuration] - [Multi-Card Opening Personnel Groups] - [Add] to show the following edit interface:

Group Name: Any combination of up to 30 characters that cannot be identical to an existing group name;

After editing, click [OK], return and the added Multi-Card Opening Personnel Group will appear in the list;

(2) Select a group and click [Add personnel] to add personnel to the group:

(3) After adding personnel, click [OK] to save and return.

Note: A person can only belong to one group and can not be grouped repeatedly.

2. Multi-Card Opening:

Set levels for personnel in [Multi-Card Opening Personnel Groups].

If [Multi-Card Opening Personnel Groups] is not configured, the system will prompt and the user can only add a combination name. The system permits the user to add a name-only combination and to edit Multi-Card Opening combination when [Multi-Card Opening Personnel Groups] is added.

Multi-Card Opening combination is a combination of the personnel in one or more Multi-Card Opening Personnel Group. When setting the number of people in each group, you can configure one group (such as combined door opening by two people in one group) or multiple groups (such as combined door opening by four people, including 2 people in group 1 and 2 people in group 2), and at least one group shall be entered a number of door opening people not being 0, and conversely the total number of door opening people shall not be greater than 5. In addition, if the number of people entered by the user is greater than the number of people in the current group, the Multi-Card Opening utility will be unable to function.

Multi-Card Opening settings:

(1) Click [Access Control System] - [Door configuration] - [Door management], click [Set] under “Multi-Card Opening” of a door in the door list to show the Multi-Card Opening setting interface;

(2) Click [Add] to pop up the Add Multi-Card Opening setting interface;

(3) For Multi-Card Opening, the number of people for combined door opening is up to 5. The number in brackets indicates the current number of people in the group. Select the number of people for combined door opening in a group, and click [OK] to complete editing.

6.3.4 Interlock Settings

Interlock can be set for any two or more lock belong to one access control panel, so that when one door is opened, the others will be closed. And you can open one door only when others are closed.

Before interlock setting, please make sure the access controller is connected with door sensor according to the Installation Guide, and the door sensor has been set as NC or NO state.

Add Interlock Settings:

1. Click [Access Control System] - [Door configuration] - [Interlock settings] - [Add] to enter the Interlock setting edit interface;

2. Select a device to show the Interlock Settings. Since one device can only correspond to one Interlock Setting Record, when adding, interlocked devices cannot be seen in the dropdown list of the device. When deleting established interlock information, the corresponding device will return to the dropdown list. The setting page will vary with the number of doors controlled by the selected device:

A one-door control panel has no interlock settings;

A two-door control panel: 1-2 two-door interlock settings;

A four-door control panel: 1-2 two-door interlock, 3-4 two-door interlock, 1-2-3 three-door interlock, 1-2-3-4 four-door interlock;

3. Select Interlock Settings, select an item (multiple interlocks can be selected as long as doors are not repeated) and click [OK] to complete the setting. The added Interlock Settings will be shown in the list.

For example, select 1-2-3-4 four-door interlock. If you want open door 3, doors 1, 2 and 4 need to be closed.

Note: When editing, the device cannot be modified but the Interlock Setting can be modified. If Interlock Setting is not required for the device any more, the Interlock Setting Record can be deleted. When deleting a device record, its Interlock Setting Record will be deleted if it exists.

6.3.5 Anti-pass Back Settings

Currently, Anti-pass Back Settings support in and out Anti-pass Back. In some special occasions, a card holder who enters a door by card punching is required to exit from the same door by card punching, with the entry and exit records strictly consistent. One who followed another to enter the door without card punching will be denied when trying to exit by card punching, and one who followed another to exit without card punching will be denied when trying to enter by card punching. When a person enters by card punching and gives the card to another to try entering, the other person will be denied. The user can use this function just by enabling it in the settings. This function is normally used in prisons, the army, national defense, scientific research, bank vaults, etc.

Add Anti-pass Back Settings:

1. Click [Access Control System] - [Door Configurations] - [Anti-pass Back Settings] - [Add] to show Anti-pass Back Setting edit interface;

2. Select a device (N-door control panel), because one device can only correspond to one Anti-pass Back Setting Record, when adding, devices with Anti-pass Back Settings cannot be seen in the dropdown list. When deleting established Anti-pass Back information, the corresponding device will appear in the dropdown list. The settings vary with the number of doors controlled by the device:

Anti-pass Back can be set between readers and between doors. If the card holder enters from door A, he must exit from door B. This function is used for channel or ticket management.

Anti-pass Back Settings of one-door control panel: Anti-pass Back between door readers;

Anti-pass Back Settings of a two-door control panel: Anti-pass Back between readers of door 1, Anti-pass Back between readers of door 2, Anti-pass Back between doors 1/2;

Anti-pass Back Settings of a four-door control panel: Anti-pass Back of doors 1-2, Anti-pass Back of doors 3-4, Anti-pass Back of doors 1/2-3/4, Anti-pass Back of doors 1-2/3, Anti-pass Back of doors 1-2/3/4, Anti-pass Back between readers of door 1, Anti-pass Back between readers of door 2, Anti-pass Back between readers of door 3, Anti-pass Back between readers of door 4.

Note: The reader mentioned above includes Wiegand reader that connects with access control panel and inBIO reader. The single door and two door control panel with Wiegand reader includes out reader and in reader. There is only an in reader for the four door control panel. The reader number of 1, 2 (that is RS485 address or device number, the same below) is for door 1, the reader number of 3, 4 is for door 2, etc. There is no need to identify whether it is a Wiegand reader or inBIO reader in setting Anti-pass Back between doors or between readers. Just make sure of the in or out state (means it is the in reader or out reader) and set according to the actual need. An odd number designates an in reader, and an even number designates an out reader.

3. Select Anti-pass Back Settings, and select one item (Anti-pass Back without repetition of doors or readers can be subject to multi-choice). Click [OK] to complete the setting. The added Anti-pass Back Settings can be shown in the list.

Note: When editing, you cannot modify the device but can modify Anti-pass Back Settings. If Anti-pass Back Settings are not required for the device any more, the Anti-pass Back Setting record can be deleted. When deleting a device record, its Anti-pass Back Setting record will be deleted, if it exists.

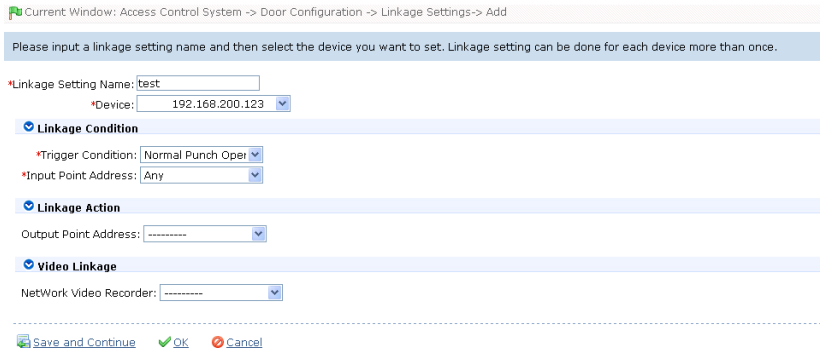
6.3.6 Linkage Setting

Linkage Setting means when an event is triggered at an input point of the Access Control System, a linkage action will occur at the specified output point to control such events as verification, opening, alarm and exception of the system and list them in the corresponding monitored report for view by the user.

Add Linkage Setting:

1. Click [Access Control System] - [Door Configurations] - [Linkage Setting] - [Add] to show the Linkage setting interface;

2. Enter a Linkage Setting Name (input Linkage Setting Name before selecting the device). After selecting the device the corresponding Linkage Setting will appear (The system will first determine whether or not the device is successfully connected and has read extended device parameters such as auxiliary input quantity, auxiliary output quantity, door quantity and reader quantity. If the system has no available extended device parameters, it will remind the user of failing to set anti-pass back. Otherwise, it will show Linkage Setting options according to the currently selected device, such as the door quantity, auxiliary input and output quantity):


Current Window: Access Control System -> Door Configuration -> Linkage Settings-> Add
Please input a linkage setting name and then select the device you want to set. Linkage setting can be done for each device more than once.
*Linkage Setting Name: test
*Device: 192.168.200.123
Linkage Condition
*Trigger Condition: Normal Punch Oper
*Input Point Address: Any
Linkage Action
Output Point Address: ---------
Video Linkage
NetWork Video Recorder: ---------
Save and Continue
OK
Cancel

The fields are as follows:

Trigger Condition: Please refer to 6.6 Real-time Monitoring for the Real Time Events Description. Except Linkage Event Triggered, Cancel Alarm, Open Auxiliary Output, Close Auxiliary Output, and Device Start, all events could be trigger condition.

Input Point Address: Any, Door 1, Door 2, Door 3, Door 4, Auxiliary Input 1, Auxiliary Input 2, Auxiliary Input 3, Auxiliary Input 4, Auxiliary Input 9, Auxiliary Input 10, Auxiliary Input 11, Auxiliary Input 12 (for the specific input point please refer to specific device parameters);

Output Point Address: Lock 1, Lock 2, Lock 3, Lock 4, Auxiliary Output 1, Auxiliary Output 2, Auxiliary Output 3, Auxiliary Output 4, Auxiliary Output 6, Auxiliary Output 8, Auxiliary Output 9, Auxiliary Output 10 (the specific output point please refer to specific device parameters);

Action Type: Close, Open, Normal Open. By default it is closed. To open, the delay time must be set or Normal Close can be selected;

Delay: Ranges from 1-254 seconds (This item is valid when the action type is Open)

Network Video Recorder: Select the network video recorder;

Bound Channel: Select the bound channel, channel 1-8 is optional.

Note: The Network Video Recorder function is only available for professional version 5.0.8 and above. If you need to use the Network Video Recorder, please contact our commercial representative or sales support.

3. After editing, click [OK] to save and quit and the added linkage setting will be shown in the linkage setting list.

For example: If you select “Normal Punching Card Open” as the trigger condition, and the input point is Door 1, the output point is Lock 1, the action type is Open, and the delay is 60 seconds, then when “Normal Punching Card Open” occurs at Door 1, the linkage action of “Open” will occur at Lock 1, and door will be open for 60 seconds.

Note: When editing, you cannot modify the device but can modify Linkage Setting name and configuration. When deleting a device, its Linkage Setting Record will be deleted, if it exists.

If the system has setting that the input point is a specific door or auxiliary input point under a trigger condition of a device, it will not allow the user to add (or edit) a Linkage Setting Record where the device and trigger condition are the same but the input point is ‘Any’.

Conversely, if the device and trigger condition are the same, and the system has a Linkage Setting Record where the trigger point is ‘Any’, the system will not permit the user to add (or edit) a Linkage Setting Record where the input point is a specific door or auxiliary input.

In addition, the system does not allow the same Linkage Setting at an input point and an output point in a specific trigger condition.

The same device permits consecutive logical (as mentioned above) Linkage Settings.

Video linkage includes hard linkage and soft linkage. The hard linkage is the same as the previous description. The system will synchronize the setting information to access control panels. The access control panel (no matter if it is offline or online) can execute the current linkage setting. The soft linkage is only applicable to the video linkage. After the system obtains a particular real-time event from the access control panel, you can use the software to query the video data from the hard disk and play on the interface.

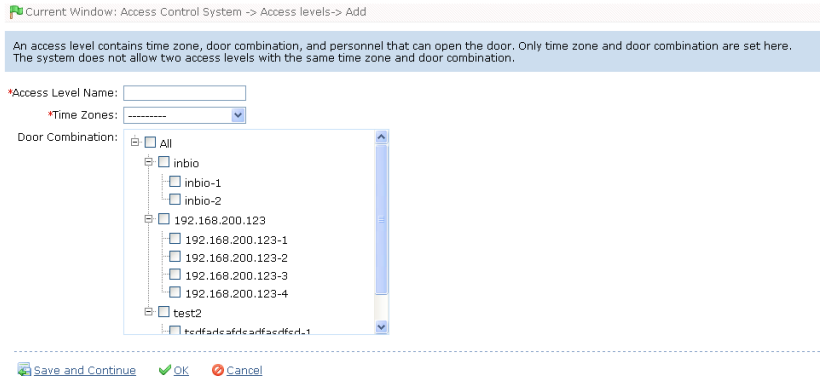
Note: The video linkage function is only available for professional version 5.0.8 and above. If you need to use the video linkage function, please contact our commercial representative or sales support.

6.4 Access Levels

Access Levels means in a specific time period, which door or door combination can be opened through verification. However, the personnel combination that can open these doors via verification shall be set in Personnel Access Levels Settings. Please refer to 6.5 Personnel Access Levels settings.

Add Access Levels:

1. Click [Access Control System] - [Access Levels] - [Add] to enter Add Access Levels edit interface;



2. Set parameters: Access Level Name (no repetition), Access Control Time Zones, Door Combination;

3. Click [OK] to complete the setting and quit. The added access levels will appear in the list.

Note:

(1) Select the doors in the Access Levels as multi-choice, so you can select different doors in different control panels;

(2) Two levels with the same time zone and door combination are not allowed in the system.

6.5 Personnel Access Levels

To assign access levels for personnel to verify and pass through, Personnel Access Levels have two display modes:

Show by Access Levels: Add/delete personnel for specific access levels.

Show by Personnel: Add specified personnel into specified access levels, or delete specified personnel from specified access levels;

1. Add/Delete Personnel to Levels:

(1) Click [Access Control System] - [Personnel Access Levels] - [Shown by Access Levels], click a level, then personnel having opening levels in the access level will be shown in the list on the right;

(2) Click [Add Personnel] to open the Add Personnel interface, select personnel to create the list on the right, and click [OK] to

complete adding. The added personnel will appear in the list on the right;

(3) Select personnel, click [Delete from Access Level] to delete the personnel from the access level.

Note: When adding personnel, if selected personnel exist in the current access level, the system cannot them add again.

2. Edit Access Level for Personnel:

(1) Click [Access Control System] - [Personnel Access Level Settings] - [Shown by Personnel] interface, click a person, and the list on the right will show the access level of that person;

(2) Click [Add Access Level] to open the edit interface, select access level, and click [OK] to complete editing. The list on the right will show the access level;

(3) Select access level and click [Delete Access Level] to delete the person from the access level.

6.6 Real-time Monitoring

Monitor the statuses and real-time events of doors under the access control panels in the system in real-time, including normal events and exceptional events (including alarm events).

1. Monitoring All:

The system will, by default, show the monitoring of all doors under the control panels within the current user's access level. The user can monitor one (or more) doors by [Area], [Control Panel] or [Door].

Remote Opening/Closing: Including the operations of single door and all current doors. In single door operation, move the cursor to the door icon, click [Remote Opening/Closing] in the popup menu. In all current doors operation, click [Close All Current Doors] in the main interface to fulfill the operation.

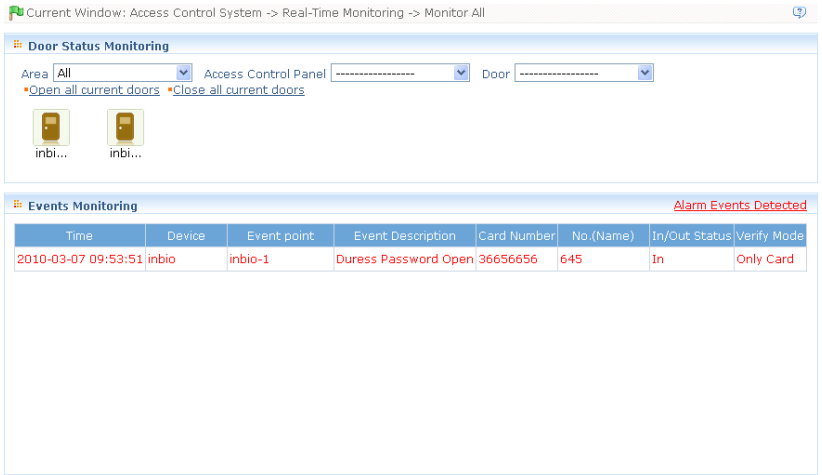
When you remote close the door, the open time interval is enabled15 seconds by default. You can select [Enable Intraday Normal Open Time Zone], and the Normal Open Time Zone Intraday will take effect. You can also set the door state to Normal Open directly, and no time zone intraday can affect the door state any more (namely normally open for 24 hours).

If you want to close the door, select [Disable Intraday Normal Open Time Zone] first to avoid other normal open time zones taking effect and opening the door. Then select [Remote Closing] to complete the operation.

Note: If the operations of remote opening/closing always return failure, please check the current list of devices. If there are too many offline devices, you need to check the network to ensure the operation progressed normally.

Cancel all alarms: Once alarming doors appear on the interface, the system will alarm. Click to cancel the alarms of the control panels for alarming doors. If Cancel Alarms is successful, the system will automatically stop alarming.

Note: If a control panel has multiple door alarms at the same time, you only need to execute one cancel operation at one of these doors to cancel all the alarms in this control panel.



Upon Door Status Monitoring, if the number of doors on the current interface ≤64, the system will, by default, show the doors in pictures to monitor door statuses. Once the number exceeds 64, the system will automatically list the doors.

When putting the cursor on a door, it will show relevant parameters and operations: device, door number, door name, remote opening, and remote closing. Icons in different colors represent statuses as follows:

Icon							
Status	Door alarming	Door closed when online	Door opened when online	Door sensor unset	Device banned	Door Offline	Door opening timeout

Personnel Photo Display:

If there is a person of concern in the Real-time Monitoring and the corresponding photo is set prior, the photo will be displayed in Real-time Monitor. And the event name, trigger time, person name will be displayed on the photo.

Event Monitoring:

The system automatically acquires monitored device event records, including normal access control events and exceptional access control events (including alarm events). Alarm events appear in red. Exceptional events excluding alarm events appear in orange. Normal events appear in green.

Presently, when an alarm event record appears on the event monitoring interface, the “Find alarm event” prompt will appear on the upper right corner. After the user clicks the link, the system will redirect to the alarm event monitoring interface by opening a new window (or tab page).

On the current event monitoring interface, the recent records are on the top, enabling the user to see without dragging the scrollbar. Currently, the interface shows up to 50 records.

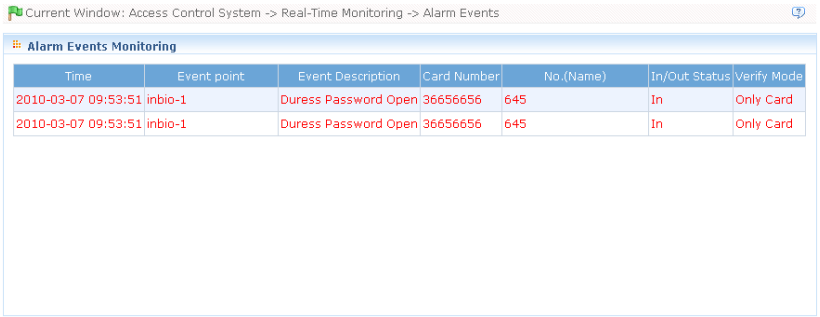
Click [Find Alarm Event] on the upper right corner to access the [Alarm Event] interface and the user will see alarm events monitored in [Event Monitoring] before page turn and alarm events after the current time point.

2. Alarm Event:

Alarm Event records are actually part of Exception records, namely, Alarm Event records in Exception records.

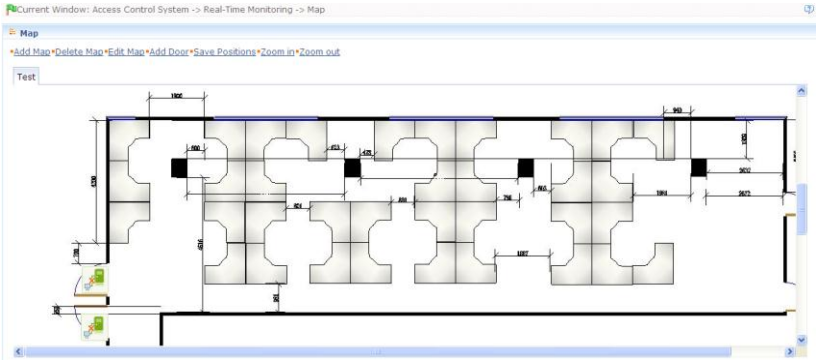
Alarm Event Monitoring only monitors alarm events acquired in the system and only monitors alarm events after the time of accessing the interface.

The Alarm Event Monitoring list is shown below:



3. Electro-Map

Before using the Electro-Map, the user needs to add the map to the system. After successfully adding, the user can add doors, zoom-in and zoom-out on the map (and on the door on the map), etc. If the user changes the door icon, or the map, or the position of door icon, click [Save Position] to save the current position, then the user can view the setting at the next time it is accessed.


Current Window: Access Control System -> Real-Time Monitoring -> Map
Map
Add Map Delete Map Edit Map Add Door Save Positions Zoom in Zoom out
Test

Add Map and **Delete Map:** The user can add or delete the map as needed.

Edit Map: The user can change the map name, change the map or change the area it belongs to.

Adjust Map (includes door): The user can add a door on the map or delete an existing one (right click the door icon, and select [Remove Door]), adjust the map or position of the door icon (by drag the door icon), or adjust the size of the map (click [Zoom in] or [Zoom out]).

Real-time Door Status Monitoring: Except to display the Electro-Map, the system views the Real-time Event Monitoring (same data source with door status monitoring, including alarm sound, etc.).

Door Operation: Move the mouse icon to the door position, the system will automatically filter the operation according to the door status and display them on the popup menu. The user can remote open or close the door, cancel alarm, etc.

User Rights Control:

(1) In the adding process, the user needs to select an area on the map. The area set here is relevant to the user management rights. That is, the user can only view or manage the map under his rights. If the user modifies an area of a map, all doors on that map will be cleared, and needs to be added again.

(2) When the administrator adds a new user, he can manage the user operation rights by role setting, such as the operations of [Save Door Position], [Zoom in], [Zoom out], etc.

Note:

(1) In map modification, the user can select to modify the map name but not the path. They only need to cancel the tick before [Modify Path].

(2) The system supports adding multi door at the same time. After door adding, the user needs to set the door position on the map and click [Save] after setting.

(3) When modifying a door position, zoom in on the map. The margin in the upper left should not be smaller than 5 pixels. The system will prompt an error if the margin is smaller.

(4) The system recommends adding a map size under 1120 pixels x 380 pixels. If the multi clients access the same server, the display effect will differ according to the resolution of the screen and the browser settings.

Appendix: Real-time Event Description (the fingerprint events are only available for version 5.0.8 and above):

1. Normal Events:

Normal Punch Open: In [Card Only] verification mode, the person has open door permission, punch the card and trigger this normal event of open the door.

Press Fingerprint Open: In [Fingerprint Only] or [Card plus Fingerprint] verification mode, the person has the open permission, press the fingerprint at the valid time period, the door is opened and triggers the normal event.

Card plus Fingerprint Open: In [Card plus Fingerprint] verification mode, the person has the open permission, punch the card and press the fingerprint at the valid time period, the door is opened and triggers the normal event.

Exit Button Open: User presses the exit button to open the door within the door valid time zone and triggers this normal event.

Punch During Normal Open Time Zone: At the normally open period (set to normally open period of a single door or the

door open period after the first card normally open), or through the remote normal open operation, the person has open door permission, punch the effective card at the opened door to trigger this normal event.

Press Fingerprint During Normal Open Time Zone: At the normally open period (set to normally open period of a single door or the door open period after the first card normally open), or through the remote normal open operation, the person has open door permission, press the effective fingerprint at the opened door to trigger this normal event.

First Card Normal Open (Punch Card): In [Card Only] verification mode, the person has first card normally open permission, punch card at the setting first card normally open period but the door is not opened, and trigger the normal event.

First Card Normal Open (Press Fingerprint): In [Fingerprint Only] or [Card plus Fingerprint] verification mode, the person has first card normally open permission, press the fingerprint at the setting first card normally open period but the door is not opened and triggers the normal event.

First Card Normal Open (Card plus Fingerprint): In [Card plus Fingerprint] verification mode, the person has first card normally open permission, punch the card and press the fingerprint at the setting first card normally open period but the door is not opened and triggers the normal event.

Normal Open Time Zone Over: After the setting normal open time zone, the door will close automatically. The normal open time zone includes the normal open time zone in door setting and the selected normal open time zone in first card setting.

Remote Normal Opening: Set the door state to normal open in the remote opening operation and trigger this normal event.

Cancel Normal Open: Punch the valid card or use remote opening function to cancel the current door normal open state and trigger this event.

Disable Intraday Normal Open Time Zone: In door normal open state, punch the effective card five times near the card reader (must be the same user), or select [Disable Intraday Normal Open Time Zone] in remote closing operation and trigger this normal event.

Enable Intraday Normal Open Time Zone: If the intraday door normal open time zone is disabled, punch the effective card five times near the card reader (must be the same user), or select [Enable Intraday Normal Open Time Zone] in remote opening operation and trigger this normal event.

Multi-Card Open (Punching Card): In [Card Only] verification mode, multi-card combination can be used to open the door. After the last card is verified, the system triggers this normal event.

Multi-Card Open (Press Fingerprint): In [Fingerprint Only] or [Card plus Fingerprint] verification mode, multi-card combination can be used to open the door. After the last fingerprint is verified, the system triggers this normal event.

Multi-Card Open (Card plus Fingerprint): In [Card plus Fingerprint] verification mode, multi-card combination can be used to open the door. After the last card plus fingerprint is verified, the system triggers this normal event.

Multi-Card Open (Press Fingerprint): In [Card Only] verification mode, multi-card combination can be used to open the door. After the last fingerprint is verified, the system triggers this normal event.

Multi-Card Open (Card plus Fingerprint): In [Card Only] verification mode, multi-card combination can be used to open the door. After the last card plus fingerprint is verified, the system triggers this normal event.

Emergency Password Open: The password (also known as the super password) set for the current door can be used for door open. It will trigger this normal event after the emergency password is verified.

Open during Normal Open Time Zone: If the current door is set a normally open period, the door will open automatically after the setting start time and trigger this normal event.

Linkage Event Triggered: After the system linkage configuration takes effect, this normal event is triggered.

Cancel Alarm: When the user cancels the alarm of the corresponding door and the operation is a success, this normal event is triggered.

Remote Opening: When the user opens a door by remote and the operation is successful, it will trigger this normal event.

Remote Closing: When the user closes a door by remote and the operation is successful, it will trigger this normal event.

Open Auxiliary Output: In linkage action setting, if the user selects Auxiliary Output for Output Point Address and selects Open for Action Type, it will trigger this normal event when the linkage setting takes effect.

Close Auxiliary Output: In linkage action setting, if the user selects Auxiliary Output for Output Point Address and selects Open for Action Type, it will trigger this normal event when the linkage setting takes effect and if the user closes the opened auxiliary output through the [Close Auxiliary Output] operation in [Door Setting], this normal event triggers too.

Door Opened Correctly: When the door sensor detects that the door has been properly opened, this normal event is triggered.

Door Closed Correctly: When the door sensor detects that the door has been properly closed, this normal event is triggered.

Auxiliary Input Disconnected: When the auxiliary input point is disconnected, this normal event is triggered.

Auxiliary Input Shorted: When the auxiliary input point is short circuited, this normal event is triggered.

Device Start: When the device starts, this normal event is triggered.. This event cannot be displayed on the real-time monitor but it can be checked in the event report.

2. Abnormal Events

Too Short Punch Interval: When the interval between two card punches is less than the set time interval, this abnormal event is triggered.

Too Short Fingerprint Pressing Interval: When the interval between two card punches is less than the set time interval, this abnormal event is triggered.

Door Inactive Time Zone (Punch Card): In [Card Only] verification mode, the user has the door open permission and punches the card but not within the door effective period of time, this abnormal event is triggered.

Door Inactive Time Zone (Press Fingerprint): The user has the door open permission and presses the fingerprint but not within the door effective period of time, this abnormal event is triggered.

Door Inactive Time Zone (Exit Button): The user has the door open permission and punches the card but not within the access effective period of time, this abnormal event is triggered.

Illegal Time Zone: A user with permission to open the current door punches the card during the invalid time zone triggers this abnormal event.

Access Denied: A registered card without access permission for the current door punches to open the door triggers this abnormal event.

Anti-pass Back: When the Anti-pass Back Setting of the system takes effect, this abnormal event is triggered.

Interlock: When the interlocking rules of the system take effect, this abnormal event is triggered.

Multi-Card Authentication (Punching Card): Use Multi-Card Combination to open a door, the card verification before the last one (whether verified or not), triggers this normal event.

Multi-Card Authentication (Press Fingerprint): Use Multi-Card Combination to open a door, the fingerprint verification before the last one (whether verified or not), triggers this normal event.

Multi-Card Authentication (Punching Card): Use Multi-Card Combination to open a door, the card verification before the last one (whether verified or not), triggers this normal event.

Multi-Card Authentication (Press Fingerprint): In [Fingerprint Only] or [Card plus Fingerprint] verification mode, use Multi-Card Combination to open a door, the fingerprint verification before the last one (whether verified or not), triggers this normal event.

Unregistered Card: If the current card being used is not registered in the system, this abnormal event is triggered.

Unregistered Fingerprint: If the current fingerprint is not registered or it is registered but not synchronized with the system, this abnormal event is triggered.

Opening Timeout: If the door sensor detects that the delay time after open has expired, the door is closed and this abnormal event is triggered.

Card Expired: The person with the door access permission punches the card to open the door after the effective time of the access control and cannot be verified, this abnormal event will trigger.

Fingerprint Expired: The person with door access permission presses fingerprint to open the door after the effective time of the access control and cannot be verified, this abnormal event will trigger.

Password Error: Use Card plus Password, Duress Password or Emergency Password to open the door, this event is triggered if the password is wrong.

Failed to Close during Normal Open Time Zone: If the current door is in normal open state but the user can not close the door through [Remote Closing] operation, this abnormal event is triggered.

3. Emergency Events

Duress Password Open: When the Duress Password of the current door is verified, this alarm event is triggered.

Opened Accidentally: Except for all the normal events (such as user with door open permission to punch card and open the door, password open door, open the door at normally open period, remote door open, the linkage triggered door open), the door sensor detects the door is opened unexpectedly.

Duress Fingerprint Open: When the duress fingerprint of the current door is verified, this alarm event is triggered.

6.7 Access Control Reports

Includes [All Access Control Events], [Access Control Exception Events] and [Personnel Access Levels] reports. You can select Export all and Export after query.

The user can generate statistics of relevant device data from access control reports, including card verification information, door operation information, and normal card punching information, etc.

For more information on Normal events and Abnormal events, please refer to 6.6 Real-time Monitoring.

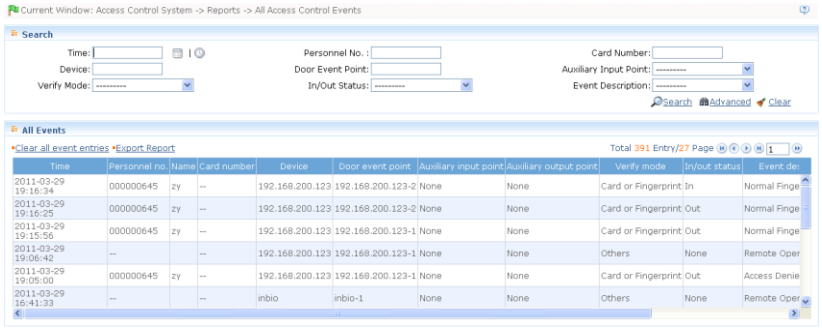
Abnormal Event: Too Short Punch Interval, Door Inactive Time Zone (Punch Card), Door Inactive Time Zone (Exit Button), Illegal Time Zone, Access Denied, Anti-pass Back, Interlock, Multi-Card Authentication, Unregistered Card, Opening Timeout, Card Expired, Password Error, Failed to Close during Normal Open Time Zone, Duress Password Open, Opened Accidentally, and Duress Password Open and Opened Accidentally are emergency events.

Verify Mode: Only Card, Only Password, Only Fingerprint, Card plus Password, Card plus Fingerprint, Card or Fingerprint and etc.

Note: Only event records generated when the user uses emergency password to open doors will include [Only Password] verification mode.

❁ All Access Control Events

Because the data size of Access Control Event Records is large, you can view Access Control Events for specified conditions when querying. By default, the system shows the report for all Access Control Events:


Current Window: Access Control System -> Reports -> All Access Control Events
Search
Time:
Personnel No. :
Card Number:
Device:
Door Event Point:
Auxiliary Input Point:
Verify Mode:
In/Out Status:
Event Description:
Search
Advanced
Clear
All Events
Clear all event entries
Export Report
Total 391 Entry/27 Page
Time
Personnel no.
Name
Card number
Device
Door event point
Auxiliary input point
Auxiliary output point
Verify mode
In/out status
Event de:
2011-03-29 19:16:34 000000645 zy -- 192.168.200.123 192.168.200.123-2 None None Card or Fingerprint In Normal Finge
2011-03-29 19:16:25 000000645 zy -- 192.168.200.123 192.168.200.123-2 None None Card or Fingerprint Out Normal Finge
2011-03-29 19:15:56 000000645 zy -- 192.168.200.123 192.168.200.123-1 None None Card or Fingerprint Out Normal Finge
2011-03-29 19:06:42 -- -- 192.168.200.123 192.168.200.123-1 None None Others None Remote Oper
2011-03-29 19:05:00 000000645 zy -- 192.168.200.123 192.168.200.123-1 None None Card or Fingerprint Out Access Denie
2011-03-29 16:41:33 -- -- inbio inbio-1 None None Others None Remote Oper

Clear All Event Records:

Click [Clear All Event Records] to open a prompt. Click [OK] to clear records.

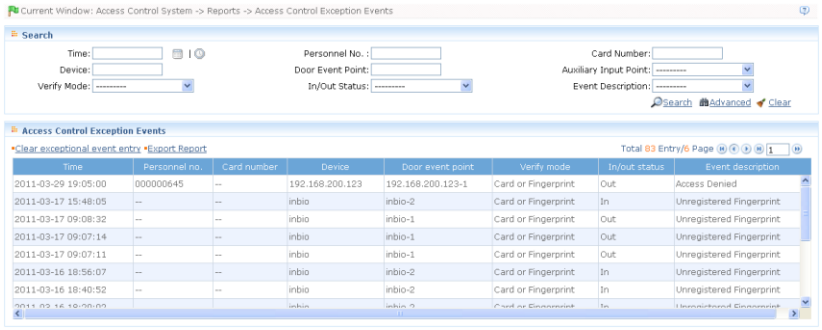
Set the Time for Obtaining New Entries:

Click [Set the Time for Obtaining New Entries] to open a time-setting dialog, and click [OK] to finish setting after inputting the time.

Note: The user should ensure that the server is powered on for the time set. The software can only obtain new entries on the hour and the time range is 0-23. After finishing, the user will need to restart the software services by using [Services Controller], or the server to submit the change.

❁ Access Control Exception Events

You can view Access Control Exception Events for specified conditions. The options are same as those of [All Access Control Events].

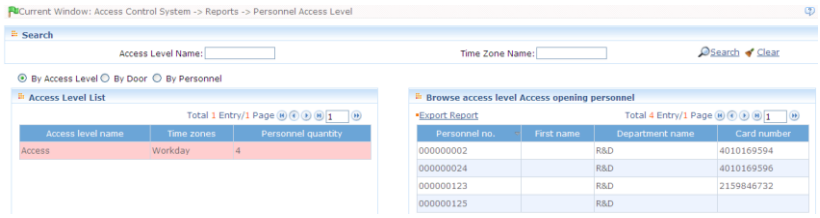

Current Window: Access Control System -> Reports -> Access Control Exception Events
Search
Time:
Device:
Verify Mode:
Personnel No. :
Door Event Point:
In/Out Status:
Card Number:
Auxiliary Input Point:
Event Description:
Search
Advanced
Clear
Access Control Exception Events
Clear exceptional event entry
Export Report
Total 83 Entry/6 Page
Time
Personnel no.
Card number
Device
Door event point
Verify mode
In/out status
Event description
2011-03-29 19:05:00 000000645 -- 192.168.200.123 192.168.200.123-1 Card or Fingerprint Out Access Denied
2011-03-17 15:48:05 -- -- inbio inbio-2 Card or Fingerprint In Unregistered Fingerprint
2011-03-17 09:08:32 -- -- inbio inbio-1 Card or Fingerprint Out Unregistered Fingerprint
2011-03-17 09:07:14 -- -- inbio inbio-1 Card or Fingerprint Out Unregistered Fingerprint
2011-03-17 09:07:11 -- -- inbio inbio-1 Card or Fingerprint Out Unregistered Fingerprint
2011-03-16 18:56:07 -- -- inbio inbio-2 Card or Fingerprint In Unregistered Fingerprint
2011-03-16 18:40:52 -- -- inbio inbio-2 Card or Fingerprint In Unregistered Fingerprint

Clear Access Control Exception Event Records: Clear the list of all Access Control Exception Events.

❁ Personnel Access Level

View all Access Levels according to access level group, door or personnel. Select the query mode and the condition in the left data list. The corresponding result will display in the right data list.

For example, select “By Access Level”, the data list on the left side shows all access levels. Select an access level. The personnel under this access level will display in the right data list.



7. Video System (For Professional Version 5.0.8 and above)

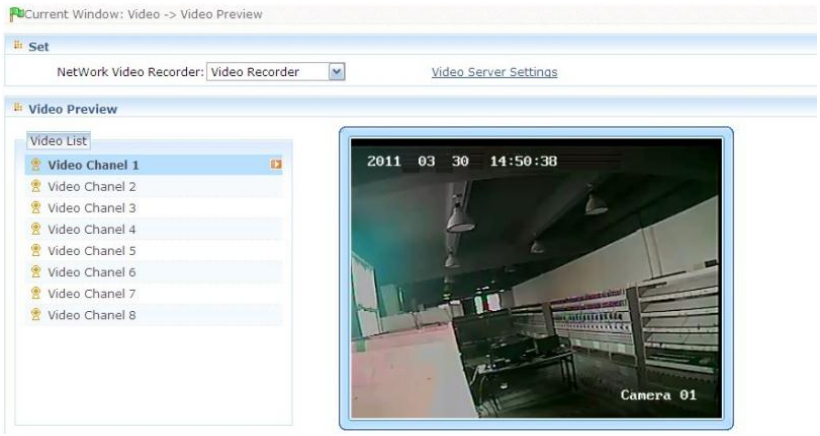
The system provides video linkage function to manage the network video recorder, view the Real-time Video, query the video record and open the Real-time Video when the Linkage Events happened.

Before using the video linkage function, the user needs to add a network video recorder. For detailed operation, please refer to 5.2.2 Add Network Video Recorder. After adding, the user needs to set video linkage in linkage settings (set the network video recorder and bound channel), then the user can view the real-time monitor video in the system. For detailed settings, please refer to 6.3.6 Linkage Setting.

Note: The current software version only supports Hikvision embedded network DVR, such as DS-91xx series, DS-81xx/71xx/72xxHV series, DS-80xx/70xx/72xxH series, and DS-78xx/88xx series. The recommended model is DS-7808H-ST-AF-DVR-II-B/.8-4. For other models to use in the system, please contact a Hikvision technician.

Video Preview:

Enter [Video]-[Video Preview], open the video preview interface, select the preview channel to view the remote preview image.

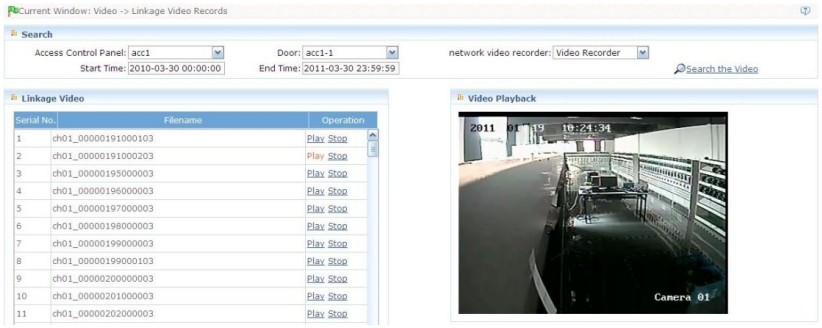


Double click the image to enter the full screen mode.

Double click the image, or click [Windows] icon on your keypad, or press Ctrl+ESC to exit the full screen mode.

Linkage Video Records:

Enter [Video]-[Linkage Video Records] to query or playback the linkage video records.



Select the corresponding control panel, door or network video recorder, input the start and end time and click the [Search the Video] button. If the record matches the condition, the record number and name will display on the list and the play and stop operation is permitted.

Click the [Play] button and the video will playback on the right interface. Click [Stop] to stop it.

See the description above for full screen operation.

Alarm Preview:

After setting the linkage event, if the Real-time Linkage Event happens, the preview interface will open in the Real-time Monitor interface.

8. System Settings

System Settings primarily include assigning system users (such as company management personnel, registrar, access control administrator) and configuring the roles of corresponding modules, managing databases, such as backup, initialization, and setting system parameters and operation logs, etc.

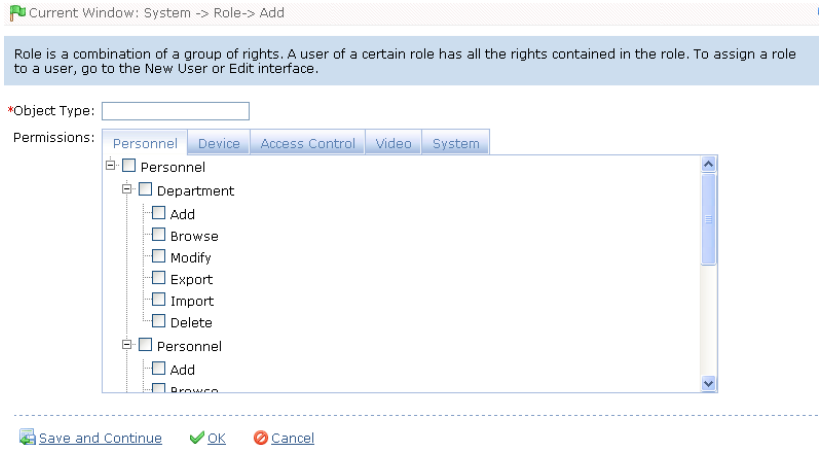
8.1 User Management

1. Role Management:

During daily use, the super user needs to assign new users having different levels. To avoid individual settings for each user, roles having certain levels can be set in Role Management, and then be assigned to specified users, including the levels set for five major functional modules; personnel, device, access control, video system and system setting. The system's default super user has all levels, and can create new users and set corresponding levels as required.

Role Setting Steps:

(1) Click [Add] to enter Role setting interface;



(2) Set Role Name, select your desired role setting item, and tick levels to be configured for users of different levels;

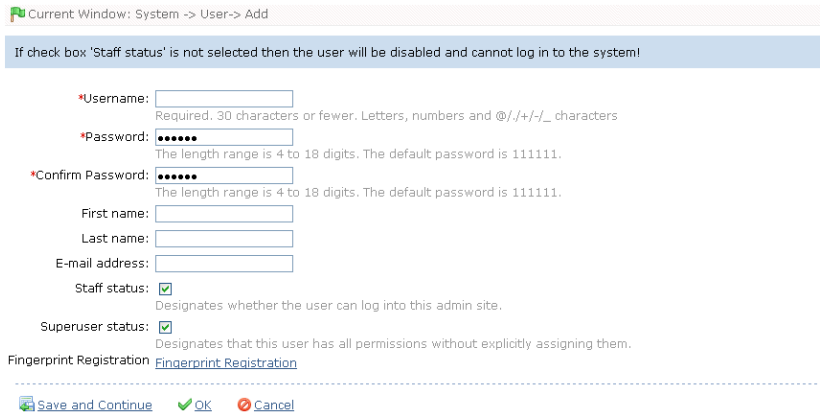
(3) After setting, click [OK] to save and return to the list, and added role settings will be shown in the list.

2. User Management:

Add new users to the system, and assign user roles (levels).

Add User:

1. Click [Add], enter new user information, where items with [*] are mandatory. The parameters are as follows:


Current Window: System -> User-> Add
If check box 'Staff status' is not selected then the user will be disabled and cannot log in to the system!
*Username:
Required. 30 characters or fewer. Letters, numbers and @/./+/-/_ characters
*Password:
The length range is 4 to 18 digits. The default password is 111111.
*Confirm Password:
The length range is 4 to 18 digits. The default password is 111111.
First name:
Last name:
E-mail address:
Staff status:
Designates whether the user can log into this admin site.
Superuser status:
Designates that this user has all permissions without explicitly assigning them.
Fingerprint Registration
Fingerprint Registration
Save and Continue
OK
Cancel

Username: Not more than 30 characters, using only letters, numbers or characters;

Password: The length must be more than 4 digits and less than 18 digits. The default password is 111111;

Authorize Department: If you select no department, you will possess all department rights by default;

Authorize Area: If you select no area, you will possess all area rights by default;

Enter **First Name**, **Last Name** and **E-mail Address**;

Staff Status: Indicates if this user can access the administrator site;

Super User Status: Designates that this user has all permissions without explicitly assigning them. Tick it to be a super user without selecting a role;

Select **Role:** Non-super user needs to select a role. By selecting a preset role configuration, this user will have the levels configured for the role.

Fingerprint Registration: Enroll the user fingerprint or duress fingerprint. The user can login the system by pressing the enrolled fingerprint. If the user presses the duress fingerprint, it will trigger the alarm and send the signal to the system.

2. After editing, click [OK] to complete user adding. The user will be shown in the list.

To modify an existing user, click [Edit] behind the User Name, and enter the edit interface. After modification, click [OK] to save and return.

8.2 Database Management

The homepage of the system shows database backup history. The system allows database backup, restoration and initialization.

1. Database backup path configuration:

Select [Database Backup Path Configuration] in the [Server Controller] operation menu. The edit interface appears.

Click [Browse] to select the backup path, click [Save] to save the selection and quit.

Note:

(1) In the software installation process, it will prompt to set the database backup path. If you have not set the backup path, the operation of backup database cannot be executed (The backup path in the server must be set before other computers can access the server).

(2) It is recommended that the database backup path and the present system installed path not be on the same disk. Don't set the path to the root of a disk, and no blanket permitted.

2. Backup Database:

Periodically backup the system's database to ensure data security. To use the backed up data, just restore the data.

(1) Click [Backup Database] to enter the Backup interface;

(2) Select the operation: backup now, scheduled backup and cancel scheduled backup. Scheduled backup can set backup to run on planned dates and times;

(3) Click [OK] and the system will open the database backup path prompt. For Backup now, it will return after backup. For scheduled backup, it will backup as scheduled.

Note:

(1) After database backup, the value under “Whether backup successful” will change to “Yes” or “No”. “Yes” indicates database backup was successful, otherwise, the backup operation failed.

(2) We recommended backing up the database after you create the personnel file, device information or part of access control level settings.

(3) The system does not support backup of Oracle databases, if you need to backup, please use the specific Oracle backup tools.

3. Restore Database

Select [Restore Database] in the **[Server Controller]** operation menu, the Restore Database interface appears.

Click [Browse] to select a successfully backed up database from the backup database list, click [Start] to begin the database restoration.

Note:

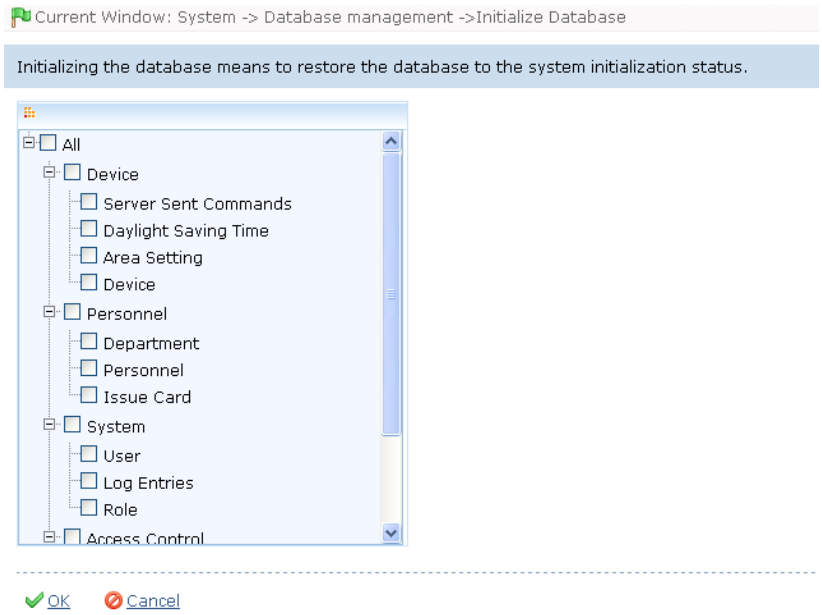
(1) Don’t close any command window prompt during the database restore process.

(2) Do not plan multiple scheduled backups on the same server to avoid adding to the server load.

4. Initialize Database:

Initialize Database is to restore data to system initialization status. Initialized data in the database will be deleted. Please operate with care.

Click [Initialize Database] to enter the edit interface. Select one or more datasheets to initialize and click [OK] to complete initialization and return.



For example:

Select to initialize Access Level: After selection, it will initialize Access Control Time Periods, Access Control Holidays and Access Levels. All contents on these three pages will restore initial statuses;

Select to initialize door settings: After selection, it will initialize all Interlock Settings, Anti-pass Back Settings, Linkage Settings, First-Card Opening Settings, and Multi-Card Opening Settings (including personnel group of Multi-Card verification);

Select to initialize events: After selection, it will initialize all Real-time Monitoring Records;

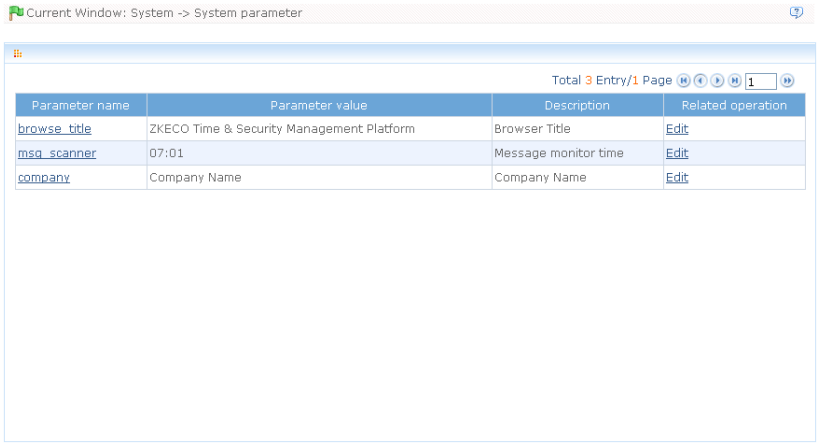
Select to initialize Access Control: After selection, it will initialize all settings and information in the Access Control System, including the above three items, and only reserve system default settings;

Select to initialize devices: After selection, it will initialize all device information in the system (including Access Control). If the device is an access control panel, corresponding device parameters and door information will be deleted.

Note: If the device is still in normal use, please initialize the database cautiously, especially when involving access level-related departments and personnel, access levels, door settings, areas, devices, users and roles. It is recommended that if there are still devices in use after database initialization, the user shall [Synchronize All Data] for the setting to avoid unexpected errors.

8.3 System Parameters

The system homepage shows the system parameter list: Parameter Name, Parameter Value, Description, and Related Operation.



8.4 Log Records

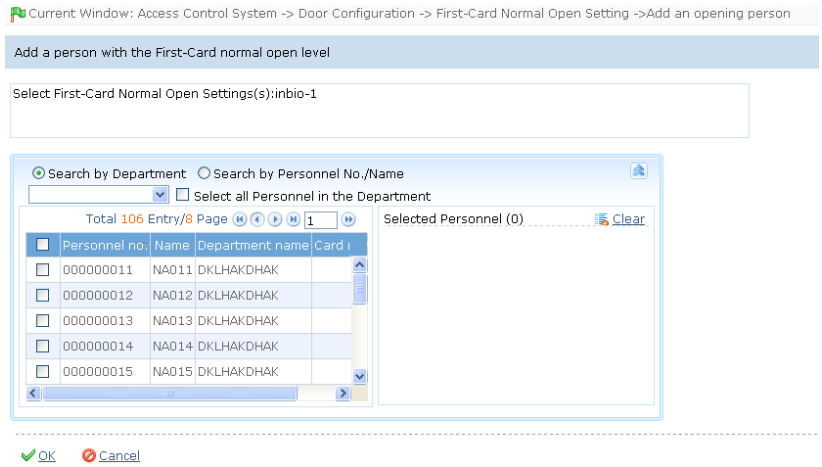
The default homepage of system Log Records shows log records of all operations. Because of the large data size, you can use the query function to search the desired log records. For details, see Appendix 1 Common Operation.

9. Appendices

Appendix 1 Common Operation

1. Personnel Selection

In this system, this dialog box is used for all modules using Personnel Selection:



You can search personnel in two ways:

1) Search by department. Tick the check box in front of a department in the department list of the pull-down menu to select all personnel in the department. If [Select All Personnel Under the Department] is ticked, all personnel in the department will be selected and shown in the list box of the currently selected personnel;

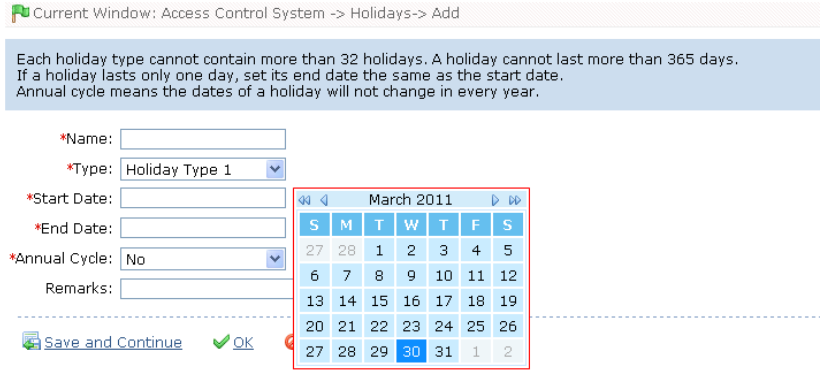
2) Search by personnel number/name. Enter the name or employee number of the desired person in the query box, and click query to show the appropriate person in the list box.

When personnel are selected in the list box, if it is required to delete one or more persons, uncheck the box in front of the person. To select or unselect all personnel in the list, click the 'Select all' check box under the list.

To cancel all personnel for reselection, click Clear.

2. Select Date

Click the pull-down menu to select date:


Current Window: Access Control System -> Holidays-> Add
Each holiday type cannot contain more than 32 holidays. A holiday cannot last more than 365 days.
If a holiday lasts only one day, set its end date the same as the start date.
Annual cycle means the dates of a holiday will not change in every year.
*Name:
*Type:
Holiday Type 1
*Start Date:
*End Date:
*Annual Cycle:
No
Remarks:
March 2011
S M T W T F S
27 28 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 1 2
Save and Continue
OK

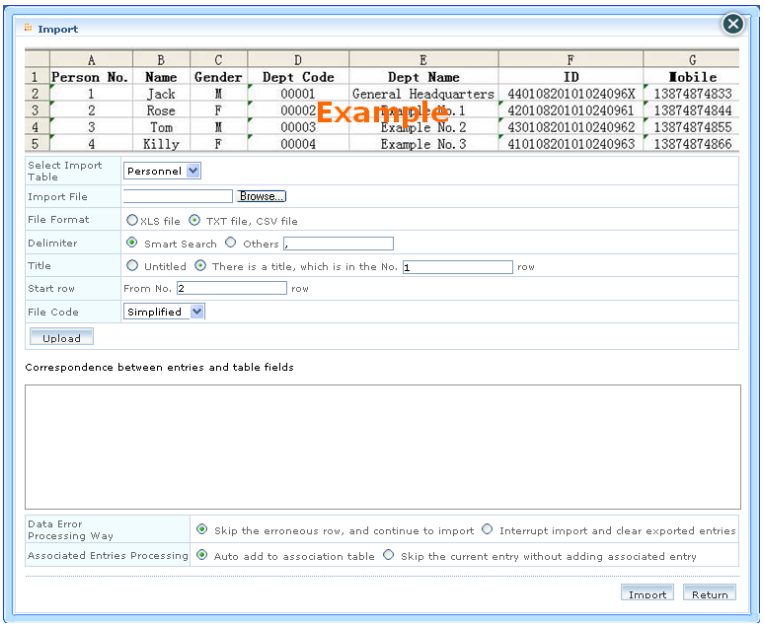
Click on the year to activate the scroll button for year selection, and click or button to select an earlier or a later year. Click or button to select an earlier or a later month then click the desired date.

3. Import (importing personnel table for example):

If there is an electronic personnel file that may be used to populate the personnel or access control, attendance or human

resources system of another brand, you can import it into this system through the [Import] function.

(1) Click [Import] to show the Import edit interface:



Description of items:

Select Import Table: Currently the system supports the import of a department table and personnel table;

Import file: Click [Browse] to select the file to be imported;

File Format: Select the format of the file to be imported;

Delimiter: The user selects from Smart Search or others, such as comma, semicolon or blank;

Title: Select and specify whether or not the original file contains a title. If so, enter which row the title is in;

Start Row: The row from which importing starts (specifically, which row of the original file the data of the first row is in);

File Code: Select the code that the original file uses, being Simplified Chinese, Traditional Chinese or utf8;

Data Error Processing Way: Select “skip the erroneous row, and continue to import”, or “interrupt import and clear imported entries”;

Associated Entry Processing: Select “auto add to associate table” or “skip the current entry without adding associated entry”.

(2) Click [Browse] to select the file to be imported;

(3) Click [Open] and the file format will be automatically shown. Determine delimiter, title, start row and file code, and click [Upload] to display the uploaded file items.

(4) In the table [correspondence between entries and table fields], [file header] is an item row in the original file, [file record] is a data row in the original file, [table field] is an item in the current system. Select corresponding fields in the system from pull-down menus. Unwanted data can be unchecked.

(5) Select data error processing way and associated entry processing, click [Import], and the system will automatically start importing data. When the system prompts that data import is successful, the newly imported data will be shown in the personnel list.

Note:

(1) When importing department table, repeated numbers do not affect import, and can be modified manually;

(2) When importing personnel table, if there is no personnel number or the personnel number is “0”, the import operation

cannot execute. If you need to import the personnel gender, please use “M” to represent male and “F” to represent female, then execute the import operation.

4. Export Data (exporting personnel list for example):

(1) Click [Export] to show the edit interface;

When the data size is large, it is recommended to select [Select Number of Entries to Export] to expedite export and reduce system load.

(2) Select the format of exported file: If PDF format is selected there will be no file code option (namely, no differentiation between Simplified and Traditional Chinese). Click [Export] to directly show the exported file.

If TXT or CSV format is selected, then file codes include Simplified and Traditional Chinese, but Traditional Chinese code can only be completely exported in the operating system in Traditional Chinese. The system prompts Open or Save:

Select [Open] to show the list. Select [Save] to open the [Save as] dialog box. Enter a file name and save type and select the save path. Select [Cancel] to return.

(3) Return to the initial edit interface, and click [Return] to return to the personnel interface.

Note:

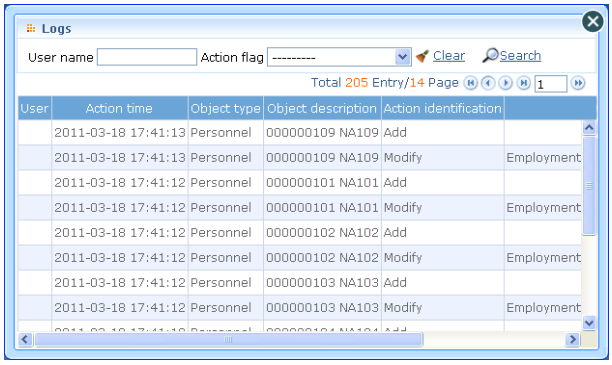
(1) When importing department table, repeated numbers do not affect import, and can be modified manually;

(2) Exported table is the list currently shown, the list of queried or displayed results;

(3) Up to 10,000 records can be exported.

5. View Log Records (personnel log for example):

(1) Click log records to show the following:



(2) Enter query conditions, click [query] to show the list. Click [Clear], clear query conditions, and return to the initial interface.

Note:

1. The log records only show the operation log in the current operation module;

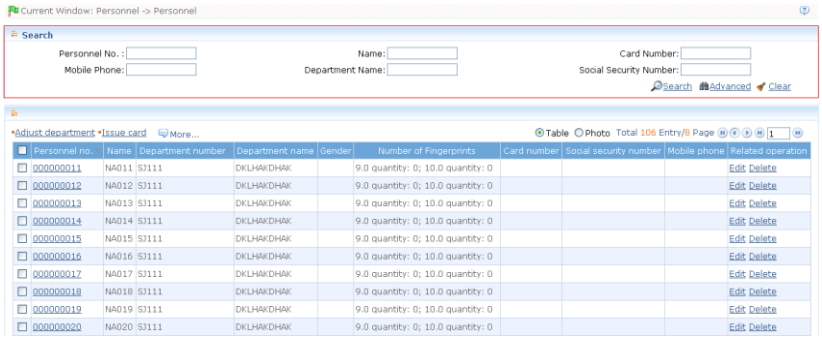
2. Log records under some operation menus can be viewed only when entering the edit interface.

For example, from [Access Control System] - [Door Configuration] - [Door Management], click [Edit] under “Related Operation” of a device to enter the edit interface, and click [Log Records] on the upper right corner of the interface to view the operation log.

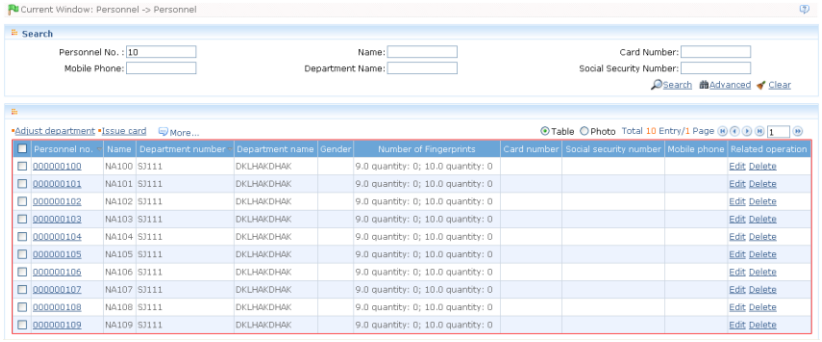
6. Query Function (personnel information query for example):

Common Query: The user can directly select the item to be queried from [Common Query] on My Work Panel, or enter a module for a specific query.

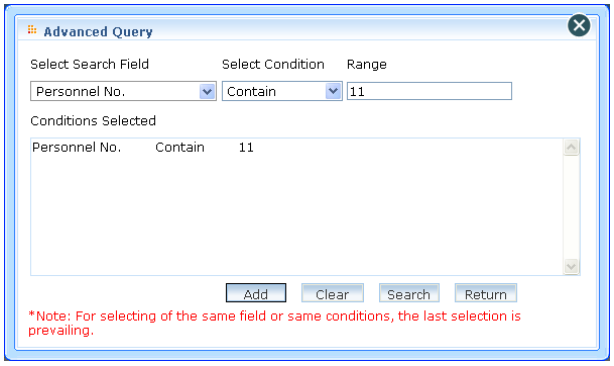
Take personnel query for example:


Current Window: Personnel -> Personnel
Search
Personnel No. :
Name:
Card Number:
Mobile Phone:
Department Name:
Social Security Number:
Search
Advanced
Clear
Adjust department
Issue card
More...
Table
Photo
Total 106 Entry/8 Page
Personnel no.
Name
Department number
Department name
Gender
Number of Fingerprints
Card number
Social security number
Mobile phone
Related operation
000000011 NA011 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000012 NA012 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000013 NA013 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000014 NA014 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000015 NA015 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000016 NA016 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000017 NA017 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000018 NA018 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000019 NA019 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000020 NA020 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete

Enter the query condition, click Query, and the query result will be shown:


Current Window: Personnel -> Personnel
Search
Personnel No. : 10
Name:
Card Number:
Mobile Phone:
Department Name:
Social Security Number:
Search
Advanced
Clear
Adjust department
Issue card
More...
Table
Photo
Total 10 Entry/1 Page
Personnel no.
Name
Department number
Department name
Gender
Number of Fingerprints
Card number
Social security number
Mobile phone
Related operation
000000100 NA100 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000101 NA101 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000102 NA102 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000103 NA103 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000104 NA104 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000105 NA105 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000106 NA106 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000107 NA107 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000108 NA108 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete
000000109 NA109 S1111 DKLHAKDHAK 9.0 quantity: 0; 10.0 quantity: 0 Edit Delete

Advanced Query: Click [Advanced] icon to show advanced query interface (using personnel information advanced query as an example).



(1) Select the query field in the [Select Query Field] pull down menu;

(2) Select the condition in the pull down menu such as equal to null, contain, meet any, equal to etc.

(3) Input the query value in the [Range] field;

(4) Click [Add] to add this query information to the [Selected Condition] list, the multiple choice of the query condition is allowed. But a field and a condition can only be selected once.

Click [Query], the query result displays in the list.

The query functions of each menu in the system are similar, differing in that the query conditions are different and the user can

enter as prompted.

Appendix 2 END-USER LICENSE AGREEMENT FOR THIS SOFTWARE

Important – please read carefully:

This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and the mentioned author of this software for the software product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. This EULA grants you the following rights: Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.

Reproduction and Distribution

You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Limitations on Reverse Engineering, De-compilation, and Disassembly

You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

Separation of Components

The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one computer.

Software Transfer

You may permanently transfer all of your rights under this EULA, provided the recipient agrees to the terms of this EULA.

Termination

Without prejudice to any other rights, the Author of this Software may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

Distribution

The SOFTWARE PRODUCT may not be sold or be included in a product or package which intends to receive benefits through the inclusion of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT may be included in any free or non-profit packages or products.

3. COPYRIGHT.

All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by the Author of this Software. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may install the SOFTWARE PRODUCT on a single computer provided you keep

the original solely for backup or archival purposes.

LIMITED WARRANTY

NO WARRANTIES.

The Author of this Software expressly disclaims any warranty for the SOFTWARE PRODUCT. The SOFTWARE PRODUCT and any related documentation is provided "as is" without warranty of any kind, either express or implied, including, without limitation, the implied warranties or merchantability, fitness for a particular purpose, or non-infringement. The entire risk arising out of use or performance of the SOFTWARE PRODUCT remains with you.

NO LIABILITY FOR DAMAGES.

In no event shall the author of this Software be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this product, even if the Author of this Software has been advised of the possibility of such damages.

Acknowledgment of Agreement

I have carefully read and understand this Agreement, Radiate, Inc.'s Privacy Policy Statement.

IF YOU ACCEPT the terms of this Agreement:

I acknowledge and understand that by ACCEPTING the terms of this Agreement.

IF YOU DO NOT ACCEPT the terms of this Agreement

I acknowledge and understand that by refusing to accept these terms, I have rejected this license agreement and therefore have no legal right to install, use, or copy this Product or the Licensed Software that it incorporates.

Appendix 3 FAQs

Q: How can My Work Panel be unique?

A: The user can customize the work panel: 1. Click [Custom Work Panel] to open a dialog box, cancel the tick of your undesired module (by default the system ticks all), and Confirm. Then the custom module will appear; 2. Or directly click the "—" icon on a module to minimize, and click "✕" to close the module. Click the column bar to drag and adjust the module's position; 3. If required to return to the default work panel, click [Restore Work Panel] to refresh and return to the system default.

Q: How is a card issuer used?

A: Connect the card issuer to the PC through USB port, and then select individual personnel card issue or batch card issue. Move the cursor to the card number input box, and punch the card on the card issuer, then the card number will be automatically shown in the input box.

Q: What is the use of role setting?

A: Role setting has the following uses: 1. To set unified level for the same type of users newly added, just directly select this role when adding users; 2. When setting system reminder, and determine which roles can be viewed.

Q: How do I set accounts for all personnel of the company's financial department?

A: First, create a new role in system setting and configure the functions to be used for this role. Then add a user, set user information, and select the user's role, thus adding a new account. For other accounts, do the same.

Q: What is the use of blacklist?

A: A blacklisted person cannot gain departure restoration, more specifically, this person cannot be employed by the Company any longer. To modify, just modify departure information on the departure interface.

Q: How do I modify a person's department?

A: There are the following ways to adjust personnel department: 1. In personnel list, click personnel number or click "Edit" under related operation item to show personnel details, and modify personnel department in the department item; 2. In personnel list, check the personnel requiring department adjustment, click "Adjust department", and a dialog box will open, then modify the department; 3. On personnel transfer interface, click Add to open the edit interface, select personnel, and check department in the transfer field, and complete the other information, thus completing the transfer.

Q: How do I set access levels for visitors?

A: Setting access levels is as follows: 1. In the system, add these personnel, and enter relevant information; 2. Select access levels suitable for them. If there are no suitable levels, it is required to enter the access control system to add relevant settings; 3. Set valid time, namely, the start and end dates when they need to use access levels.

Q: How can I cancel personnel access control settings?

A: There are the following ways to cancel personnel access control settings: 1. Close access control only: In the personnel list, click personnel number or click "Edit" under related operation item to show personnel details, and delete access levels and Personnel Group of Multi-Card Verification in access control settings; 2. Delete personnel: In the personnel list, click "Delete" under related operation item of personnel, or tick a personnel and click the "Delete" above to delete this person from the system. Corresponding access control information will be deleted; 3. In "Personnel access levels settings", delete access levels of personnel, and in "Personnel Group of Multi-Card Verification", delete Multi-Card Opening levels.

Q: How do I set access control holidays?

A: Access control holidays have three types; 1, 2 and 3. Use New Year's Day for example: 1. In access control holidays, add a holiday of "New Year's Day". Set the holiday type as 1, and the start and end dates of the holiday are both January 1; 2. During the access control time period, add an access control time zone, set the three access control intervals of this holiday type 1. For example, set access control interval 1 as 8:00-20:00, and intervals 2 and 3 as null, namely Normal Close; 3. Apply this access control time zone to access levels; 4. Set personnel with levels for the access levels.

Q: In Windows Server 2003, why does IE browser display an error when the system is accessed, how can I solve it?

A: This problem occurs because Server 2003 has [Security Configuration Option] settings. If you want access the system, configure it as follows: click Start – Control Panel – Add or Remove Program, select [Add and remove Windows components] in the interface and click [Internet Explorer Enhanced Security Configuration] option, cancel the tick before it. Click [Next] to

remove it from the system. Open the system again and the browser will access the system properly.

Q: If backing up or restoring the database fails, what is the possible reason?
A: Please check the system environment variables [path], if the database installation path exists (For example, MS SQL Server installation path maybe is: C:\Program Files\Microsoft SQL Server\90\Tools\Binn; For MySQL, it is like: C:\Program Files\MySQL\MySQL Server 5.1\bin). If not, you need to add it manually. Otherwise, the antivirus or firewall software may stop the execution of backing up or restoring command. If the security prompt opens, select “Always Permitted”. The damaged database can also lead to a backup error, repair or restore the database.